

BROCADE



EDUCATION SOLUTIONS

BCNP in a Nutshell Study Guide for Exam 150-220

Exam Preparation Materials

日本語参考版

(※注: 本スタディガイドは参考和訳です。正式な内容については本社サイトに掲載のドキュメントを参照ください。)

Revision February 2010

Corporate Headquarters - San Jose, CA USA

T: (408) 333-8000

info@brocade.com

European Headquarters - Geneva, Switzerland

T: +41 22 799 56 40

emea-info@brocade.com

Asia Pacific Headquarters - Singapore

T: +65-6538-4700

apac-info@brocade.com

© 2010 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the Brocade B-weave logo, Fabric OS, File Lifecycle Manager, MyView, Secure Fabric OS, SilkWorm, and StorageX are registered trademarks and the Brocade B-wing symbol and Tapestry are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON is a registered trademark of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

Revision: February 2010

BCNP in a Nutshell First Edition



Objective: The BCNP Nutshell guide is designed to help you prepare for the BCNP Certification, exam number 150-220.

Audience: The BCNP Nutshell self-study guide is intended for those who have successfully completed the CNE 103 (formerly ETH 103) Basic Switch Router Configuration and Maintenance course along with the ETH 405 Advanced Switch Router Configuration and Maintenance course, and who wish to undertake self-study or review activities before taking the actual BCNP exam. The BCNP guide is not intended as a substitute for classroom training or hands-on time with Brocade products.

How to make the most of the BCNP guide: The BCNP guide summarizes the key topics on the BCNP exam for you in an easy to use format. It is organized closely around the exam objectives. We suggest this guide be used in conjunction with our free online knowledge assessment test - CNP 101-WBT Brocade Certified Network Professional Knowledge Assessment. To benefit from the BCNP guide, we strongly recommend you have successfully completed the ETH 103 & ETH 405 classes.

We hope you find this useful in your journey towards BCNP Certification, and we welcome your feedback by sending an email to jcannata@brocade.com.

Helen Lautenschlager
Director of Education Solutions

Joe Cannata
Certification Manager

A handwritten signature in black ink that reads "Helen Lautenschlager".

A handwritten signature in blue ink that reads "Joe Cannata".

目次

1 - QoS 及び Voice の導入	7
レート制限(Rate Limiting)	7
レート・シェーピング(Rate Shaping)	7
トラフィックのクラス分け 及び QoS.....	8
クラス分けされたトラフィックの処理	8
QoS Queues	10
トラフィック・ポリシーの検証	10
VoIP	12
PoE.....	12
2- セキュリティの概念	13
MAC ポートのセキュリティ	13
802.1X ポート・セキュリティ.....	13
認証中の 802.1X メッセージ交換	14
一般のセキュリティ概念	15
デバイスへのユーザアクセス制御	15
アクセス制御リスト(ACL)	15
番号(Numbered)及び名前(Named)による ACL.....	16
AAA.....	17
3 - OSPF の概念.....	18
OSPF.....	18
OSPF Hello パケット	18
隣接関係(Adjacency)	18
ネイバと隣接関係の確立プロセス.....	18
OSPF 自律システム、エリア及びルータのタイプ.....	19
OSPF LSA のタイプ	19
リンクステートのコスト	20
OSPF 仮想リンク	21
ルートの再配布	22
外部ルートの集約	22
4 - BGP の概念.....	24
EBGP マルチホップ	24
IBGP ピアリングに対するループバック・インタフェイスの使用	24
マルチパス EBGP	24
ピア・グループ	25
ルート・リフレクタ	25
コンフィデレーション	26
ネクスト・ホップ・セルフ(Next-Hop-Self).....	26
BGP テーブル	27
ルーティング・テーブル	28
AS パス	28
BGP ネイバとルート情報の概要を表示する便利なコマンド	28
5- アドバンスド・レイヤ3 の概念	29

デフォルト・ルートの生成.....	29
IP ルートの選択及び管理ディスタンス	29
ルートの再配布.....	30
IPv6	30
IPv6 アドレスのタイプ	31
PIM Sparse モード(PIM-SM).....	31
IGMP スヌーピングの概要.....	31
VRRP 及び VRRP-E の比較.....	32
レイヤ 2 及びレイヤ 3 のマルチキャスト・アドレス・マッピング	33
PBR	34
6 - レイヤ2 プロトコル.....	35
MRP.....	35
RSTP ブリッジ及びブリッジ・ポートの役割	38
DHCP スヌーピング.....	40
スパニング・ツリー・プロトコル (STP)	41
BPDU ガード.....	41
LLDP.....	42
デュアル・モードの VLAN ポート.....	42
Q-in-Q.....	45
VLAN.....	45
プライベート VLAN.....	46
7 - モニタリング、メンテナンス、トラブルシューティング.....	49
OSPF 外部ルートの集約.....	49
OSPF 内部ルートの集約	49
BGP ルート・フラップ・ダンペニング	50
OSPF ネットワーク・タイプと DR/BDR の選出	51
OSPF インタフェイス: パッシブ及び無視(Ignore)	52
BGP ルートの動的更新と BGP ポリシ変更の適用	53
より多くの VLAN または仮想ルーティング・インタフェイスに対するメモリの割り当て	54
ログに対する OSPF の Syslog メッセージの指定	55
ポート・ミラーリング及びモニタリング	55
SNMP	56
パスワード・リカバリ.....	57

図一覧

図 1: パケットの Trust レベル.....	9
図 3: 802.1X メッセージ交換.....	14
図 4: IPv6 アドレス・フォーマット.....	30
図 5: マルチキャスト・アドレスのレイアウト.....	33
図 6: メトロ・リングの例.....	35
図 7: 複数のメトロ・リング.....	36
図 8: インタフェイスを共有している複数の MRP リング.....	37
図 9: デュアル・モードの VLAN ポート.....	43
図 10: デュアル・モードのポート.....	44
図 11: Q-in-Q タギング.....	45
図 12: プライベート VLAN.....	47

表一覧

表 1: QoS キュー.....	10
表 2: パワー・クラス.....	12
表 3: VLAN 及び仮想ルーティング・インタフェイスの最大値.....	54

1 – QoS 及び Voice の導入

レート制限(Rate Limiting)

インバウンド・レート制限をかける場合、受信ポートに最大値(Kbps)を指定します。コマンド例を以下に示します。

```
FastIron(config)#interface ethernet 0/2/1
FastIron(config-if-e10000-0/2/1)#rate-limit input fixed 1000000
Rate Limiting on Port 0/2/1 - Config: 1000000 Kbps, Actual: 1000000 Kbps
```

上記、固定レート制限ポリシーをかけると、インタフェイス 0/2/1、10-GbE ポートに最大 1,000,000 キロビット/秒のトラフィックを受信できます。この 1 秒間隔内で設定値を超えると、次の 1 秒間隔が始まるまで、すべてのインバウンド・パケットを破棄します。

アウトバンド・レート制限をかける場合、送信ポートに最大値(Kbps)を指定します。

- ポート・ベース (Port-based) – 各物理ポート、またはトランク・ポート上で、アウトバンド・トラフィックを指定レートで制限します。最大レートを超えたトラフィックは破棄されます。あるポートに対して 1 ポート・ベースのみ、アウトバンド・レート制限ポリシーが適用できます。
- ポート及びプライオリティ・ベース (Port- and priority-based) – 各物理ポート、またはトランク・ポート上の 802.1p プライオリティ・キューごとに、レートを制限します。指定レートを超えたトラフィックは破棄されます。1 つのポートに対して 1 つだけのプライオリティ・ベースのレート制限ポリシーをプライオリティ・キューごとに適用できます。つまり、1 つのポートに最大 8 ポート・8 プライオリティ・ベースのポリシーが設定できます。

以下の通り、ポート・ベースでレート制限をかける例を示します：

```
FastIron(config)#interface ethernet 0/1/34
FastIron(config-if-e1000-0/1/34)#rate-limit output fixed 65
Outbound Rate Limiting on Port 0/1/34 Config: 65 Kbps, Actual: 65 Kbps
```

上記、固定レート制限ポリシーをかけると、インタフェイス 0/1/34 から 65 キロビット/秒のトラフィックを送信できます。この 1 秒間隔内で設定値を超えると、次の 1 秒間隔が始まるまで、すべてのアウトバンド・パケットを破棄します。

レート・シェーピング(Rate Shaping)

アウトバンド・レート・シェーピングは、ポートに流れるアウトバンド・トラフィックの帯域をポートレベルで制御します。この機能は、超過及びバーストしたトラフィックを送信前に設定した最大制限値に抑えます。つまり、パケットは利用可能なバッファに格納されてから、設定された制限値を超えないレートで転送されます。このプロセスは、隣接機器のインバンド・トラフィックに対してより優れた制御をもたらします。あるポートに対して 1 つのグローバル・レート・シェーパ、また各ポート・プライオリティ・キューに対して 1 つのレート・シェーパが指定でき、シングル・トークン方式でレート制限されます。各トークンは、1 バイトです。

トラフィックのクラス分け 及び QoS

Quality of Service (QoS) 機能は、スイッチの帯域利用に優先順位をつけるために使用されます。QoS 機能が有効な場合、トラフィックがスイッチに到達したときにクラス分けされ、設定された優先順位に基づいて処理されます。トラフィックは破棄されたり、帯域保証のために優先制御されたり、または、帯域制限オプションの影響を受けたり、いくつかの異なるメカニズムによって設定されたとおりに動作します。

トラフィックのクラス分けは、パケットを選択するプロセスです。その処理に基づいて QoS を実行するためには、QoS の情報を読み取り、パケットに優先順位を割り当てます。そのクラス分けのプロセスは、スイッチに到達するパケットに優先順位を割り当てます。これらの優先順位は、パケットに含まれる情報を元に決定されるか、スイッチに到達したパケットに割り当てられます。いったんパケット、またはトラフィック・フローがクラス分けされるとフォーワーディング・プライオリティ・キューにマッピングされます。プロセード製品の packets は 0 から 7 の 8 つのトラフィック・クラスまでクラス分けされます。より高い優先度にクラス分けされたパケットは、高い優先度でフォーワーディング処理されます。

クラス分けされたトラフィックの処理

インタフェイス上で有効になる trust level は、QoS を実行するためにデバイスが使用する QoS 情報のタイプを決定します。プロセード製品は、トラフィックがスイッチまたは、ルーティングされる場合、様々な機能の設定に基づいて trust level を確立します。その trust level は、次のいずれかになります:

- 入力ポートのデフォルト・プライオリティ
- 静的 MAC アドレス
- Layer 2 Class of Service (CoS) 値 - これは、イーサネット・フレームの 802.1p のプライオリティ値で、0 から 7 の値になります。802.1p のプライオリティは、Class of Service とも言います。
- Layer 3 Differentiated Service Code Point (DSCP) - これは、IP パケット・ヘッダ、8 ビットの DSCP フィールドの最上位 6 ビットの値で、0 から 63 までの値になります。これらの値は、RFC2472 及び 2475 で定義されています。DSCP 値は DiffServ 値とも言われます。デバイスは自動的にパケットの DSCP 値をハードウェア・フォーワーディング・キューにマッピングします。

ACL キーワード- ACL はまた、トラフィックを優先制御し、next hop へ送信する前にトラフィックに優先順位をつけられます。以下に、プロセード製品がパケットの trust level をどのように決定するかを示します:

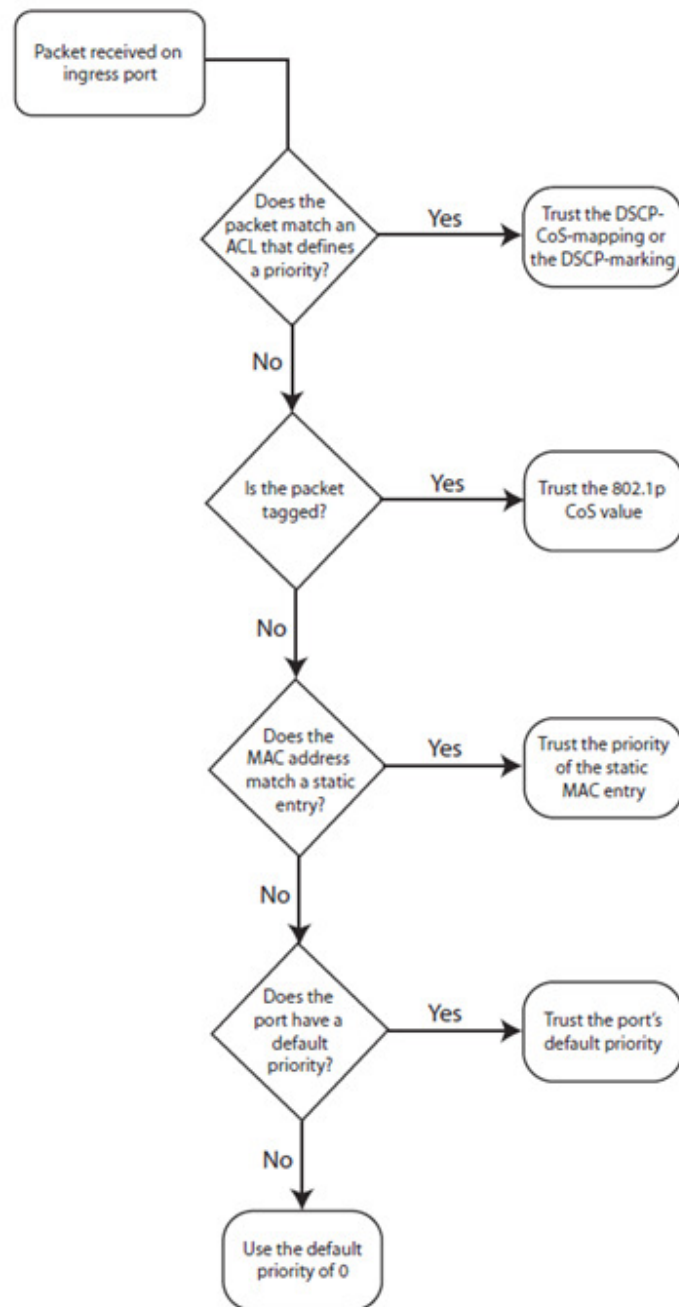


図 1: パケットの Trust レベル

最初に考慮する基準は、プライオリティを定義する ACL にパケットがマッチするかどうかになります。もし、定義した ACL にマッチせず、タグ付けされている場合、パケットは、802.1p CoS 値でクラス分けされます。定義した ACL にマッチせず、タグ付けされていない場合、パケットはスタティック MAC アドレスに基づいてクラス分けされます。スタティック MAC アドレスにもマッチしない場合は、入力ポートのデフォルト・プライオリティに、さらにどれにもマッチしない場合は、デフォルト・プライオリティゼロ(0)を使用します。

QoS Queues

ブロードのデバイスは、以上に示す 8 つの QoS キュー (qosp0 - qosp7) をサポートします:

QoSの優先度レベル	QoSのキュー
0	qosp0(最も低い優先度キュー)
1	qosp1
2	qosp2
3	qosp3
4	qosp4
5	qosp5
6	qosp6
7	qosp7(最も高い優先度キュー)

表 1: QoS キュー

トラフィック・ポリシーの検証

ブロードのデバイスに現在定義されているトラフィック・ポリシーを見るためには、show traffic-policy コマンドを入力してください。出力例を以下に示します:

```
FastIron# show traffic-policy
Traffic Policy - t_voip:
Metering Enabled, Parameters:
  Mode: Adaptive Rate-Limiting
  cir: 100 kbps, cbs: 2000 bytes, pir: 200 kbps, pbs: 4000 bytes
Counting Not Enabled
Number of References/Bindings:1
```

上記出力のフィールドの説明は以下のとおりです:

Traffic Policy: トラフィック・ポリシーの名前

Metering: レート制限がトラフィック・ポリシーの一部として設定されているかどうかを示します:

- Enabled - トラフィック・ポリシーはレート制限の設定を含みます
- Disabled - トラフィック・ポリシーはレート制限の設定を含みません

Mode: レート制限が有効な場合、このフィールドはポートで有効な測定のタイプを示します:

- 固定レート制限 (Fixed Rate-Limiting)
- 動的レート制限 (Adaptive Rate-Limiting)
- cbs: 最低帯域保証レート許容バースト設定サイズ (Committed Burst Size)、バイト毎秒、動的レート制限ポリシー
- pir: 最大情報レート (Peak Information Rate)、キロビット毎秒、動的レート制限ポリシー
- pbs: 最大帯域保証レート許容バーストサイズ、バイト毎秒、動的レート制限ポリシー

Counting: ACLトラフィック・カウントがトラフィック・ポリシーの一部として設定されているかどうかを示します:

- Enabled – トラフィック・ポリシーはACLトラフィック・カウントの設定を含みます
- Disabled – トラフィック・ポリシーはACLトラフィック・カウントの設定を含みません

Number of References/Bindings: このトラフィック・ポリシーが適用されるポート・リージョン数。例えば、もしトラフィック・ポリシーが、イーサネット・ポート9/9, 9/10, 9/11及び9/12を含むトランク・グループに適用される場合、これらの4つのトランク・ポートが異なる2つのポート・リージョンにまたがるため、このフィールドの値は、2になります。

VoIP

PoE

電力消費デバイスが接続されたポートで有効な場合、デフォルトでは、ブロードのPoEデバイスは、ケーブルによる伝送口を差し引いてRJ45ジャックで15.4ワットの電力を供給します。

電力消費デバイスに対する最大電力レベルを設定するには、以下のコマンドを入力してください:

```
FastIron#config t
FastIron(config)#interface e 1/1
FastIron(config-if-e1000-1/1)#inline power power-limit 14000
```

上記コマンドは、スロット1のイーサネット・インタフェイス1のインライン・パワーを有効にし、PoEパワーのレベルを14,000ミリワット(14 watts)に設定します。デフォルト値は、15400です。

パワー・クラスは、ブロードのPoEデバイスが電力消費デバイスに供給する最大電力を指定します。以下のテーブルは異なるパワー・クラスとそれぞれの最大電力割り当てを示します:

Class	Maximum Power (Watts)
0	15.4 (デフォルト)
1	4
2	7
3	15.4
4	29 (FCSデバイスのみ)

表 2: パワー・クラス

すべての電力消費デバイスに対するパワー・クラスのデフォルトは、ゼロ(0)です。クラス0の電力消費デバイスは、15.4ワットの電力を受信します。消費デバイスに対するパワー・クラスを設定するには、以下のコマンドを入力してください:

```
FastIron#config terminal
FastIron(config)#interface e 1/1
FastIron(config-if-e1000-1/1)#inline power power-by-class 3
```

2- セキュリティの概念

MAC ポートのセキュリティ

インタフェイス上で“信頼できる(Secure)” MACアドレスを学習するようにプロケードのデバイスを設定できます。そのインタフェイスは、学習した信頼できるアドレスに適合するソースMACアドレスの packets のみを転送します。信頼できるMACアドレスは、手動による指定、あるいは、プロケードのデバイスが自動的に学習できます。プロケードのデバイスがインタフェイスで学習できる信頼できるMACアドレス数の制限に到達した後、そのインタフェイスが学習したアドレス以外のソースMACアドレスの packets を受信した場合、セキュリティ違反とみなされます。

セキュリティ違反が生じたとき、Syslog エントリ及びSNMPトラップが生成されます。さらにそのデバイスが違反したアドレスからの packets を破棄する(また、信頼できるアドレスからの packets を許可する)か、あるいは、一定の時間、そのポートを無効にするか、いずれかのアクションを指定できます。

信頼できるMACアドレスは、インタフェイスが無効、及び再度有効になるとき、フラッシュされません。信頼できるMACアドレスは、永続的に安全に保持される(デフォルト)か、あるいは、エージアウトするよう設定できます。システムを再起動してもアドレスが安全性を維持できるように指定された間隔でstartup-configファイルに信頼できるMACアドレス・リストを自動的に保存するためにデバイスを設定できます。

ポート・セキュリティの機能は、イーサネットのインタフェイスのみに適用できます。

802.1X ポート・セキュリティ

802.1X規格は、あるネットワークにおけるクライアント/サブリカント(*Client/Supplicant*)、認証装置(*Authenticator*)、及び認証サーバ(*Authentication Server*)の役割を定義します。クライアント(802.1X規格ではサブリカント)は、ユーザ名/パスワードの情報を認証装置に提供します。認証装置は、この情報を認証サーバに送信します。クライアント情報に基づいて、認証サーバは、そのクライアントが認証装置によって供給されるサービスを使用できるかどうかを決定します。認証サーバは、この情報を認証装置に渡し、認証結果に基づいてクライアントにサービスを提供します。

認証装置(*Authenticator*) – ネットワークへのアクセスを制御するデバイスです。802.1X設定では、プロケードのデバイスが認証装置として動作します。認証装置はクライアント及び認証サーバ間のメッセージを交換します。クライアントによって供給される身元情報、及び認証サーバによって供給される認証情報に基づいて、認証装置はクライアントに対してネットワークへのアクセスを許可、または拒否します。

クライアント/サブリカント(*Client/Supplicant*) – ネットワークへのアクセスを必要とするデバイスです。クライアントは、802.1X規格をサポートするソフトウェアが稼動していないといけません(例えば、Windows XP operating system)。クライアントは、認証装置のポートに直接接続するか、あるいは、ハブを経由して接続されます。

認証サーバ(*Authentication Server*) – クライアントの正当性を確認し、クライアントがデバイス上のサービスにアクセスできるかどうかを指定するデバイスです。プロケードは、RADIUSが起動している認証サーバをサポートします。

認証中の 802.1X メッセージ交換

以下の図は、802.1Xが有効なクライアント、認証装置としてのFastIronスイッチ及び認証サーバとしてのRADIUSサーバ間のメッセージ交換のサンプルを示しています。

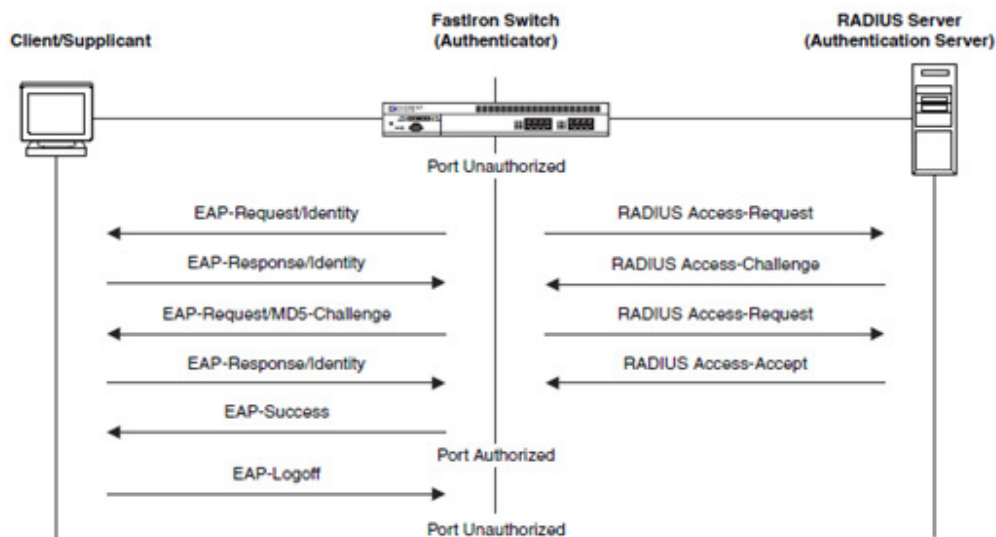


図 2: 802.1X メッセージ交換

この例では、認証装置(FastIronスイッチ)が、802.1Xが有効なクライアントとの通信を始めています。クライアントが応答するとき、ユーザ名(最大255文字)及び、パスワードが促されます。認証装置は、この情報を認証サーバに渡し、クライアントが認証装置によって提供されるサービスへアクセスできるかどうかを決定します。クライアントがRADIUSサーバによる認証に成功すると、そのポートが権限を与えられます。クライアントがログオフするとき、そのポートの権限が再度、失効します。

ブロケードの802.1Xの実装は、動的なVLAN割り当てをサポートします。もし、RADIUSサーバによって送信されたAccess-Acceptメッセージの属性のひとつがVLAN識別子を指定していて、VLANがブロケードのデバイスで有効な場合、クライアントのポートはデフォルトVLANから指定のVLANへ移動します。クライアントがネットワークから切り離されると、そのポートはデフォルトVLANに戻ります。

もしクライアントが802.1Xをサポートしていない場合、認証は動作しません。ブロケードのデバイスは、sends EAP-Request/Identityフレームをクライアントに送信しますが、クライアントは応答しません。802.1Xをサポートするクライアントが、802.1Xでない設定のポートにアクセスするとき、EAPスタート・フレームをブロケードのデバイスに送信します。そのデバイスが応答しないとき、クライアントは、権限を与えられるべきポートと見なし、通常のトラフィックを送信し始めます。

一般のセキュリティ概念

デバイスへのユーザアクセス制御

スイッチやルータへのアクセスを要求するユーザを確認するためには、以下のように、アクセスのタイプ、及び認証方法を指定する必要があります:

```
aaa authentication {アクセスのタイプ} default {確認方法}
```

設定の構文は: `aaa authentication <snmp-server|web-server|enable|login> default <method1> [<method2> <method3> <method4> <method5> <method6> <method7>]`

アクセスのタイプは Web、SNMP、Telnet 及びコンソールが選べます。確認方法は Line、Enable、Local、RADIUS、TACACS 及び TACACS+が選べます。

以下に例を示します:

```
FastIron(config)#aaa authentication login default tacacs local
```

上記コマンドは、Telnet や SSH のアクセスに対する認証方法としてはじめに TACACS や TACACS+で実行します。サーバのエラーで TACACS や TACACS+認証が失敗すると、次にローカルのユーザ・アカウントを利用して認証が実行されます。

以下に別の例を示します:

```
FastIron(config)#aaa authentication web default radius line enable
```

Web ブラウザを使用して、スイッチやルータへのアクセスを確保するために RADIUS のユーザ名を最初に使用します。もし、ユーザ名とパスワードが設定されていない、または RADIUS サーバが利用できない場合、Telnet によるパスワード"line"を使用します。もし、Telnet によるパスワードが設定されていない場合、特権ユーザ(super-user)、ポート設定(port-config)、及び、読み取り専用(read-only)パスワード"enable"を使用します。

アクセス制御リスト(ACL)

プロセードのデバイスは、ルールベースの ACL(ハードウェアベースの ACL ともいう)をサポートします。パケットの許可、または拒否の決定はハードウェアで処理されます。また、すべての許可されたパケットはハードウェアでスイッチ、またはルーティングされ、すべての拒否されたパケットはハードウェアで破棄されます。

ルールベースの ACL は、ポートに対して割り当てられた Content Addressable Memory (CAM)スペースへ、インタフェイスに割り当てた ACL エントリをプログラムします。ACL は、スタートアップのときに(または、新しい ACL が入力され、ポートに紐付けられたとき)、ハードウェアにプログラムされます。ルールベース ACL を使用するデバイスは、ACL を CAM エントリにプログラムし、パケットを許可、または拒否するために CPU 処理ではなくハードウェア処理でこれらのエントリを使用します。

ACL は、ACL ID 及び ACL エントリで構成されます:

- *ACL ID* – ACL ID は、標準 ACL は 1 から 99 までの数字です。拡張 ACL は 100 から 199 までの数字です。一連の文字・記号類(character string)も使用できます。ACL ID は個々の ACL エントリの集合を同一に扱います。ACL エントリをインタフェイスに適用するとき、ひとつひとつの ACL エントリをインタフェイスに適用せずに、インタフェイスに対する ACL エントリを含む ACL ID を適用します。これによって、大量のアクセス・フィルタ・グループ(ACL エントリ)をインタフェイスに簡単に適用することができます。
- *ACL entry* – ACL ルールとも呼ばれ、ACL ID と関連したフィルタ・コマンドです。設定できる ACL ルールの最大数は、システム全体のパラメータになり、設定しているデバイスに依存します。異なる ACL との組み合わせでエントリ最大数まで設定できます。グローバル・レベルで ACL を設定し、特定ポートの入カトラフィックに適用します。ソフトウェアは、昇順に設定された ACL エントリを適用します。条件が一致すると、ソフトウェアは ACL エントリ(パケットの許可、または拒否)に指定された行動をとり、そのパケットに対する照合をやめます。

番号(Numbered)及び名前(Named)による ACL

ACL を設定するとき数字の ID、またはアルファベット名による ACL を指定できます。番号による ACL を設定するコマンドは、名前による ACL を設定するコマンドと異なります。

- *番号による ACL* – もし数字の ID による ACL を指定する場合、標準 ACL では 1 から 99 まで、拡張 ACL では 100 から 199 までを使用できます。
- *名前による ACL* – もし名前による ACL を指定する場合、標準 ACL、または拡張 ACL を指定してから名前による ACL を指定します。

99 までの番号による標準 IP ACL、及び 99 までの番号による拡張 IP ACL を設定できます。また、99 までの名前による標準 ACL、及び 99 までの名前による拡張 ACL を設定できます。アウトバウンドではなくインバウンドに ACL を適用できます。アウトバウンドはプラットフォームによってはサポートしていません。

ACL の設定がデバイスにされていない場合、デフォルトではすべてのトラフィックを許可します。しかし、ACL を設定し、ポートに適用すると、デフォルトではそのポートに明示的に許可していないすべてのトラフィックを破棄します:

- 厳密にアクセスを制御したい場合、許可したいアクセスに対するエントリを許可する構成の ACL を設定してください。ACL は他のすべてのアクセスを暗黙的に破棄します。
- 多くのユーザをもつ環境でアクセスを確保したい場合、明示的な拒否エントリから構成される ACL を設定し、各 ACL の最後にすべてを許可するエントリを追加します。ソフトウェアは拒否エントリによって拒否されないパケットを許可します。

以下に拡張 ACL の例を示します:

```
FESX(config)# access-list 102 deny icmp any any echo log
FESX(config)# access-list 102 deny icmp any any echo-reply log
FESX(config)# access-list 102 permit icmp any any
FESX(config)# access-list 102 deny igmp host 10.10.10.10 192.168.1.0 0.0.0.255
FESX(config)# access-list 102 permit ip any any
FESX(config)# int e 1
FESX(config-if-1/1)# ip access-group 102 in
```

上記の例は、ping を拒否して他の ICMP パケットの通過を許可します。また、IP アドレス 10.10.10.10 のホストから 192.168.1.0/24 のサブネットへのビデオ・ストリームをブロックし、特別に拒否していないすべてのトラフィックの通過を許可します。

AAA

アクセス制御は、誰にネットワーク・サーバへのアクセスを許可するか、及び何のサービスの仕様を許可するかを制御する手法です。認証(Authentication)、認可(Authorization)、及びアカウンティング(Accounting) - (AAA)ネットワーク・セキュリティ・サービスは、ルータやアクセス・サーバのアクセス制御をセットアップする主なフレームワークを提供します。

- 認証(Authentication)は、ユーザとパスワードの対話、チャレンジ/レスポンス認証、メッセージング・サポート、及び暗号化(選択するセキュリティ・プロトコルに依存)を含むユーザを確認するプロセスを提供します。認証はネットワーク、及びネットワーク・サービスへのアクセスを許可される前にユーザを確認するプロセスです。
- 認可(Authorization)は、ワнтаイムの認可、または各サービス、各ユーザ・アカウントのリストとプロファイル、ユーザ・グループのサポート、IP・IPX・ARA と Telnet のサポートに対する認可を含む、リモートによるアクセス制御に対する手法を提供します。AAA 認可は、ユーザが与えられた実行権限を記述した属性群をまとめることによって動作します。
- アカウンティング(Accounting)は、ユーザの特定、時間の開始と停止、PPP のような実行コマンド、パケット数及びバイト数のような 課金、監査及びレポートに使用するセキュリティ・サーバ情報を収集及び送信する手法を提供します。

3 - OSPF の概念

OSPF

OSPF Hello パケット

すべての OSPF ルータはネイバを検知するために 224.0.0.5(All OSPF routers on this subnet)へ Hello を送信します。OSPF ネイバになるためには一定の項目が両ルータで一致しなければなりません。これらの項目は、サブネットマスク、エリア ID、Hello/Dead 間隔、認証パスワード、及びスタブ・フラグです。

隣接関係(Adjacency)

隣接関係は、ルーティング情報を交換するためにネイバ・ルータ間で関係が形成されるときに発生します。隣接関係のある OSPF ネイバ・ルータは単純な Hello パケットの交換だけではなくデータベース情報を交換します。特定のセグメントで交換する情報量を最少化するために、隣接関係を構築する最初のステップのひとつは、代表ルータ(Designated Router: 以降 DR と表記)、及びバックアップ代表ルータ(Backup Designated Router: 以降 BDR と表記)を割り当てることです。DR は隣接関係を結ぶ中心点になり、マルチアクセスのセグメントの収束時間を改善できます。直接的なレイヤ 3 接続が OSPF ルータの単一ペア間に存在する、OSPF ポイント・ツー・ポイントネットワークでは、OSPF のマルチアクセス・ネットワークで必要な DR 及び BDR は不要です。DR 及び BRD がないポイント・ツー・ポイントネットワークはより速く隣接関係を形成し、収束します。ネイバ・ルータは直接通信できるときはいつでも隣接関係を結びます。対照的にブロードキャスト、及び非ブロードキャスト・マルチアクセス(NBMA)のネットワークでは、DR 及び BDR はネットワークに接続された他のすべてのルータと隣接関係を結びます。

隣接関係はネイバリング・プロセス(単純な Down、Init 及び 2-Way 状態)の後の次のステップです。隣接関係にあるルータは、Hello の交換だけではなく、データベース交換プロセスに進んだルータです。各ルータは、DR/BDR と隣接関係を形成します。2 台のルータの LSDB がまったく同じものになるとき、隣接関係にあると言われ、"Full"なネイバ状態に到達します。OSPF ルーティングの更新は、224.0.0.6(DR/BDR routers)に対してのみ送信されます。

ネイバと隣接関係の確立プロセス

OSPF インタフェイスは別のルータと隣接関係を結ぶ前に以下のステップにより実行されます:

1. Down: セグメント上の他のルータから OSPF 情報を受信していません。
2. Attempt: フレームリレーのような NBMA(非ブロードキャストのマルチアクセス)のネットワークで、この状態はネイバから新しい情報を受信していないことを示します。ポールインタバルを減らして Hello を送信することによってネイバへコンタクトしようとします。
3. Init: インタフェイスは Hello パケットを送信します。しかし、双方向の通信は確立していません。
4. Two-way: ネイバと双方向の通信が確立されています。ルータはネイバから送信された Hello パケットの中に自分自身のルータ ID を見つけます。このステージの最後に、DR/BDR が選択されます。2-way ステージの最後に、双方のルータは隣接関係を構築するかどうかを決定します。片方のルータが DR または BDR であるかどうか、あるいはリンクがポイント・ツー・ポイントまたはバーチャルリンクかどうかに基づいて決定されます。
5. Exstart: 双方のルータは Exchange パケットで使用される最初のシークエンス番号を確立しようとします。シークエンス番号はルータが常にもっとも最新の情報を得ていることを保証します。あるルータがマスタになり、もう一方のルータがセカンダリになります。マスタはセカンダリに呼びかけて情報を交換します。
6. Exchange: 双方のルータは LSDB (リンクステート・データベース: Link-State Database) 全体を記述した DD (database description)パケットを交換します。
7. Loading: もし双方のルータのデータベースが等しくなければ、この状態になります。ルータはこの状態で情報の交換を終えます。紛失、不完全、または古くなった情報は、LSR(Link-State Request)リストにのり、ネイバに送信されます。ネイバは

LSU(Link-State Update)パケットで応えます。送信される LSU は、承認(Link-State Acknowledgement)されるまで、再送信リストにのります。

8. Full: この状態で、隣接関係が確立されます。隣接ルータは 完全な隣接関係になり、LSDB は同一になります。

OSPF 自律システム、エリア及びルータのタイプ

OSPF 自律システム (AS)は、同じ技術的管理下にあるすべての OSPF ルーティング・ドメインです。OSPF 自律システムは、複数のエリアに分けられます。リンクステータスの急激な更新に境界を設けるためにエリアを使用します。ルータのフラッディングと SPF 計算はエリア内の変更に限られます。エリアは、単一の数字または 10 進数をドットで区切った記号のどちらかで表現できます。あるエリア内のすべてのルータは、正確なリンクステート・データベースをもっています。エリア 0 はまた、バックボーン・エリアとして知られています。すべての他のエリアは、同様にバックボーン・エリアと接しています。

エリアは、インタフェイスに固有です。OSPF ルータは、複数のエリア (どれか 1 つのエリアはエリア 0 でなければならない) のメンバになれます。これらのルータは、エリア・ボーダ・ルータ(ABR)として知られています。各 ABR は、ルータが存在する各エリアに対する個別のトポロジ・データベースを維持します。各トポロジ・データベースは一定のエリア内の各ルータに対するすべての LSA データベースから成ります。同じエリア内のルータは、同一のトポロジ・データベースをもちます。ABR は、責任をもってボーダ・エリア間でルーティング情報の転送や変更を行います。

自律システム・ボーダ・ルータ(ASBR)は、他のルーティング・ドメイン内のネットワークに到達するために、複数のルーティング・プロトコルを走らせ、OSPF ルータにゲートウェイとして機能するルータです。ASBR は再配布として知られるプロセスを通じて、異なるルーティング・プロトコルから OSPF へ、ルートを注入します。ASBR は通常のエリアまたは NSSA に存在します。

OSPF LSA のタイプ

タイプ 1: ルータ LSA。所属する各エリアの各ルータによって生成されます。この LSA タイプは、コストを含むすべてのローカル OSPF インタフェイスを列挙します。それは、自エリア内にフラッディングされます。

タイプ 2: ネットワーク LSA。個々のネットワークに接続されたルータ群を記述した DR によって生成され、自エリア内にフラッディングされます。

タイプ 3: ネットワーク・サマリ LSA。エリア間ルータを記述した ABR によって生成されます。それは、他のエリアへフラッディングされます。

タイプ 4: ASBR サマリ LSA。ASBR のインタフェイス IP アドレスを広報する ABR によって生成されます。それは、ASBR に接続されていないエリアへフラッディングされます。

タイプ 5: 外部 LSA。自律システムに対する外部ネットワークまたはデフォルト・ルートを記述した ASBR によって生成されます。それは、スタブまたは NSSA でない通常のエリアにのみフラッディングされます。

タイプ 7: NSSA 外部 LSA。NSSA エリア内の ASBR によって生成されます。それは、NSSA 内のみフラッディングされます。それは、外部の送信先またはデフォルト・ルートを広報します。ABR は、バックボーン・エリア及び他の通常のエリアにフラッディングする前に、タイプ 7 をタイプ 5 に変換します。

リンクステートのコスト

OSPF が有効な各インタフェイスは、インタフェイスと関連したコストをもっています。レイヤ 3 スイッチは、そのインタフェイスとコストを OSPF ネイバに広報します。例えば、インタフェイスが、10 の OSPF コストをもつ場合、レイヤ 3 スイッチは、他の OSPF ルータに 10 のコストでインタフェイスを広報します。

デフォルトでは、インタフェイスの OSPF コストは、インタフェイスのポート速度に基づきます。コストはポート速度による参照帯域幅を等分することによって計算されます。デフォルトの参照帯域幅は、100Mbps で、以下のデフォルトのコストになります:

- 10 Mbps ポート - 10
- すべての他のポート速度 - 1 (もし結果が 1 より小さいコストの場合、ソフトウェアはコストを切り上げて 1 にします)

ソフトウェアによって計算されたコストを変更するためには、参照帯域幅を変更できます。ソフトウェアは、コスト計算に以下の計算式を使用します。: $\text{コスト} = \frac{\text{参照帯域幅}}{\text{インタフェイス速度}}$

10 Gbps の OSPF インタフェイスでは、100 Mbps、1000 Mbps 及び 10,000 Mbps インタフェイス間のコストを区別するために、参照帯域幅を 10,000 に設定して回線の帯域幅に応じて自動的に計算できます。以下のとおり、より速度の遅い各リンクは、より高いコストが与えられます:

- 10 Mbps ポートのコスト = $10000/10 = 1000$
- 100 Mbps ポートのコスト = $10000/100 = 100$
- 1000 Mbps ポートのコスト = $10000/1000 = 10$
- 10000 Mbps ポートのコスト = $10000/10000 = 1$

物理的に 1 ポート以上からなるインタフェイスに対する帯域幅は以下のとおり計算されます:

- トランク・グループ - すべてのポートを結合した帯域幅
- 仮想インタフェイス - 仮想インタフェイスを含むポート・ベース VLAN ですべてのポートを結合した帯域幅

デフォルトの参照帯域幅は、100 Mbps です。参照帯域幅の値を 1 から 4294967 に変更できます。参照帯域幅に対する変更によりインタフェイスに対するコストに変更が生じた場合、レイヤ 3 スイッチはレイヤ 3 スイッチによって広報されたインタフェイスのコストを更新するために、リンクステートの更新を送信します。

OSPF 仮想リンク

仮想リンクはトランジット・エリアを経由するバックボーンに対するエリアを接続するために使用されます。仮想リンクを設定するルールは以下の通りです:

1. 仮想リンクは 2 つの ABR 間で設定しなければなりません。ルータ ID を使用している双方のルータで設定されなければなりません。
2. 仮想リンクが設定されているエリアは、トランジット・エリアといい、バックボーン・エリアではない通常のエリア(non-backbone normal area)でなければなりません (すべてのルーティング情報を持っていないければなりません)。

すべての ABR は、OSPF バックボーン・エリア(0.0.0.0 または 0)に対して直接的または間接的なリンクをもっていないければなりません。もし ABR が物理的なリンクをバックボーン・エリアに対してもっていない場合、その ABR からバックボーン・エリアに対する物理的な接続をもつ同じエリア内の別のルータへ仮想リンクを設定できます。

バーチャルリンクに対するパスは隣の ABR(物理的にバックボーン接続をもつルータ)及びバックボーンへの論理的接続を要求する ABR によって共有されたエリアを経由します。2 つのパラメータはすべてのバーチャルリンクに対して定義されなければなりません。— トランジット・エリア ID 及びネイバ・ルータ:

- トランジット・エリア ID は、2 つの ABR の共有エリアを意味し、2 つのルータ間の接続ポイントとして動作します。この数字はエリア ID の値に一致します。
- 論理接続を要求するルータ・インタフェースから割り当てられたとき、ネイバ・ルータのフィールドはバックボーンに物理的に接続されたルータの ID(IPv4 アドレス)です。
- 物理接続をもつルータのインタフェースから割り当てられたとき、ネイバ・ルータのフィールドはバックボーンへの論理接続を要求するルータの ID(IPv4 アドレス)です。

エリア仮想リンクを確立するとき、双方のルータ(仮想リンクの両エンド)で設定しなければなりません。たとえば、バックボーン・エリア(エリア 0)から隔離された、エリア 1 及びエリア 2 をもつ ABR1 があると仮定します。ABR1 へのバックボーン・アクセスを提供するために、仮想リンクをトランジット・エリアとしてエリア 1 を使用して、エリア 1 内の ABR1 及び ABR2 の間に追加できます。仮想リンクを設定するために、リンクの各エンドにあるルータ上でリンクを定義します。トランジット・エリア内のルータで、仮想リンクに対する設定は必要ありません。ABR1 の仮想リンクを定義するためには、ABR1 で以下のコマンドを入力してください:

```
FastIron(config-ospf6-router)#area 1 virtual-link 209.157.22.1
```

ABR2 の仮想リンクを定義するためには、ABR2 で以下のコマンドを入力してください:

```
FastIron(config-ospf6-router)#area 1 virtual-link 10.0.0.1
```

OSPF 仮想リンク情報を表示するためには、CLI レベルで以下のコマンドを入力してください:

```
FastIron#show ip ospf virtual-link
```

仮想リンクの追加により、インターネットワークは複雑なレイヤになり、トラブルシューティングは難しくなります。2 つ以上のインターネットワークをマージするとき、バックボーンへの直接のリンクがないエリアが残らないように十分な計画をとるべきです。もし仮想リンクが設定される場合、避けられないトポロジの問題を修正する一時的な対処として使われるべきです。

ルートの再配布

再配布は、ASBRとして動作させるよう設定したルータで有効にしなければなりません。たとえば、RIPとスタティック IP ルートの OSPF への再配布を有効にするためには、以下のコマンドを入力してください:

```
FastIron(config)#router ospf
FastIron(config-ospf-router)#redistribution rip
FastIron(config-ospf-router)#redistribution static
```

外部ルートの集約

レイヤ 3 スイッチが OSPF の ASBR(Autonomous System Boundary Router)であるとき、特定のアドレス範囲のすべての再配布されたルートに対する集約ルートとして、ひとつの外部ルートを広告するように設定できます。

アドレス範囲を設定すると、すぐに有効になります。すべてのインポートされたルートは設定したアドレス範囲にしたがって、集約されます。すでに広告され、かつ、その範囲内にあるインポートされたルートは、その AS から消え、その範囲に相当する単一ルートが広告されます。

設定したアドレス範囲内のあるルートがレイヤ 3 スイッチによってインポートされる、レイヤ 3 スイッチがすでに集約ルートを広告している場合、新たにルート集約のアクションは行われません。もし集約ルートが広報されていないと、レイヤ 3 スイッチは集約ルートを広告します。もしアドレス範囲を指定してインポートされたルートがレイヤ 3 スイッチから削除され、なおかつ、同じアドレス範囲内を指定した他にインポートされたルートがある場合、新たにルート集約のアクションは行われません。もしインポートされたルートがない場合、集約ルートは削除されます。

集約ルートは、32 のアドレス範囲まで設定できます。レイヤ 3 スイッチは集約ルートの転送アドレスを 0 にセットし、そのタグを 0 にセットします。もしアドレス範囲を削除する場合、広告された集約ルートが消され、その範囲内のすべてのインポートされたルートが個々に広告されます。

外部 LSDB オーバフロー状態が発生する場合、すべての集約ルートは他の外部ルートとともに AS から消されます。レイヤ 3 スイッチが外部 LSDP オーバフロー状態でなくなると、すべてのインポートされたルートは設定したアドレス範囲にしたがって集約されます。

OSPF に対する集約アドレスを設定するためには、以下のようなコマンドを入力してください。

```
FastIron(config-ospf-router)#summary-address 10.1.0.0 255.255.0.0
```

この例にあるコマンドは集約アドレス、10.1.0.0 を設定しており、アドレス 10.1.1.0、10.1.2.0、10.1.3.0 などを含んでいます。これらすべてのネットワークに対して、10.1.0.0 のみが外部 LSA で広告されます。

設定した集約アドレスを表示するためには、以下のコマンドを CLI のレベルを問わず、入力してください:

```
FastIron#show ip ospf config
OSPF Redistribution Address Ranges currently defined:
Range-Address Subnetmask
1.0.0.0        255.0.0.0
1.0.1.0        255.255.255.0
1.0.2.0        255.255.255.0
```

4 - BGP の概念

EBGP マルチホップ

EBGP スピーカ、たとえば、WAN 上のリンクは通常、直接接続されていますが、リンクが直接接続されていない場合があります。この特別なケースでは、`neighbor x.x.x.x ebgp-multihop [<num>]` コマンドが使われます。`ebgp-multihop [<num>]` コマンドは、ネイバが 1 つ以上のホップで、セッション・タイプが EBGP マルチホップを示します。このオプションはデフォルトでは無効です。<num> パラメータは、ネイバに対して追加する TTL を指定します。0 から 255 までの値を指定できます。デフォルトは 0 です。EBGP TTL 値を 0 にセットする場合、ソフトウェアは IP TTL 値を使用します。マルチホップは EBGP に対してのみ使用され、iBGP に対しては使用されません。

IBGP ピアリングに対するループバック・インタフェイスの使用

ピアを確立するためにループバック・インタフェイスを使用することは、一般的に、EBGP より IBGP で使用されます。ループバック・インタフェイスは、2 つのピア間で IP 接続性がある限り、ネイバ関係が維持されることを確実にするために使用されます。

OSPF のようなローカル IGP を経由した到達性があれば、お互いのホップ数がいくつかあっても、IBGP ネイバは、AS 内の場所を問いません。複数の物理的なパスが IBGP ピア間であるかもしれません。デフォルトでは、BGP はピアへ送信するパケットの送信元アドレスとして物理インタフェイスの IP アドレスを使用します。もし物理インタフェイスがダウンすると、ピアへの別のパスがあっても、パケットを送信できないかもしれません。ピアを確立するためにループバック・インタフェイスを使用することによって、ひとつの物理リンクがダウンしたとしても、2 つのピアは他の物理リンクを経由して到達できます。

BGP ネイバの TCP 接続を起動するために物理インタフェイスよりループバック・インタフェイスを使用するように、ネイバ・ルータは BGP に伝える必要があります。BGP コマンド `neighbor x.x.x.x update-source <ip-addr> | ethernet [<slotnum>/]<portnum> | loopback <num> | ve <num>` は、特定のローカル・インタフェイスを通じてネイバと通信するようにルータを設定します。

マルチパス EBGP

デフォルトでは、BGP4 ロード・シェアリングが有効な場合、IBGP 及び EBGP 両方のパスがロード・シェアリングに対して望ましく、一方で、異なるネイバ AS からのパスはロード・シェアリングしません。IBGP または EBGP パスのみに適用するため、または異なるネイバ AS からの複数のパス内でロード・シェアをサポートするため、ロード・シェアを変更できます。

IBGP パスだけ、ロード・シェアリングを有効にする場合、次のコマンドを CLI の BGP 設定レベルで入力してください:

```
FastIron(config-bgp-router)#multipath ibgp
```

EBGP パスだけ、ロード・シェアリングを有効にする場合、次のコマンドを CLI の BGP 設定レベルで入力してください:

```
FastIron(config-bgp-router)#multipath ebgp
```

ピア・グループ

ピア・グループは共通のパラメータを共有する BGP ネイバのセットです。ピア・グループは次の利点を供給します:

- 簡単なネイバ設定 – ネイバ・パラメータ・セットを設定し、それから複数のネイバに適用できます。共通のパラメータをお互いのネイバ上で個々に設定する必要はありません。
- Flash memory conservation – 各ネイバに対するすべてのパラメータを個々に設定する代わりに、ピア・グループを使用することで、スタートアップ・コンフィグのファイル内での設定コマンドがより少なくて済みます。

ピア・グループ内のすべてのネイバ・パラメータをセットできます。ネイバをピア・グループに追加するとき、ネイバに対して明示的に設定したパラメータ値を除いて、グループ内でセットしたすべてのパラメータ設定を受信します。ここでは、ピア・グループを設定する例を示します:

```
FastIron(config-bgp-router)#neighbor PeerGroup1 peer-group
FastIron(config-bgp-router)#neighbor PeerGroup1 description"EastCoast_Peers"
FastIron(config-bgp-router)#neighbor PeerGroup1 remote-as 100
FastIron(config-bgp-router)#neighbor PeerGroup1 distribute-list out 1
```

ルート・リフレクタ

通常、AS 内部の BGP ルータはフルメッシュです。各ルータは AS 内の他のそれぞれの BGP ルータと IBGP セッションをもちます。各 IBGP ルータは、それぞれの IBGP ネイバに対するルートをもっています。多くの IBGP ルータが存在する大規模な AS に対して、各フルメッシュの IBGP ルータ内の IBGP ルート情報は、多くの管理オーバーヘッドをもたらします。

この問題を回避するために、IGP ルータを階層的にクラスタで構成します。クラスタは、ルート・リフレクタ及びルート・リフレクタ・クライアントで構成された IGP ルータのグループです。ルート・リフレクタでクラスタ ID を割り当て、そのクラスタ・メンバである IGP ネイバを識別することによってクラスタを設定できます。ルート・リフレクションに対するすべての設定は、ルート・リフレクタで行われます。クライアントは、ルート・リフレクション・クラスタのメンバであることに気づいていません。クラスタのすべてのメンバは、同じ AS 内にある必要があります。クラスタ ID は、0 から 4294967295 までのいかなる値でもかまいません。デフォルトは、ルータ ID になり、32 ビットの数字で表現されます。クラスタが複数のルート・リフレクタを含む場合、同じクラスタ ID をクラスタ内のすべてのルート・リフレクタで設定する必要があります。クラスタ ID によって、ルート・リフレクタがクラスタ内でループすることを回避します。

ルート・リフレクタは、クラスタ内のすべてのクライアント(ほかの BGP4 ルータ)へ BGP ルート情報を送信するために設定された IGP ルータです。ルート・リフレクションは、プロトコルの BGP4 ルータで有効にできますが、ルータに対してルート・リフレクタ・クライアントを追加しない限り、有効にはなりません。

ルート・リフレクタ・クライアントは、クラスタ・メンバとして識別された IGP ルータです。クライアントではなく、ルート・リフレクタであるルータ上でルータをルート・リフレクタ・クライアントとして識別します。クライアント自身は、追加の設定が必要ありません。実際に、クライアントは自分がルート・リフレクタ・クライアントであることを知りません。クライアントはただ、ネイバからの更新を受信していることを知っているだけで、複数のネイバがルート・リフレクタであるかどうかは知りません。

コンフェデレーション

コンフェデレーションは、複数の内部 AS をもつ BGP4 の自律システム(AS)です。AS 内をより小さい AS に階層化することで管理を簡素化し、BGP 関連のトラフィックを減少させ、AS 内の BGP ルータ間の IBGP フルメッシュの複雑性を減少させます。

各 BGP ルータは AS 内のすべての BGP ルータへの iBGP 接続をもつために、AS 内のすべての BGP ルータは、フルメッシュ構成になります。これは、より小規模な AS 内では現実的ですが、たくさんの BGP ルータを含む大規模な AS 内では管理が困難です。

コンフェデレーション内の BGP ルータを設定するとき、サブ AS(AS の細分化した一部)内のすべてのルータは、IGP を使用し、フルメッシュでなければなりません。そして、ルータは、異なるサブ AS 間には EBGP を使用します。

コンフェデレーションを設定するためには、サブ AS 内で BGP のグループを設定してください。サブ AS は単なる AS です。サブ AS という用語は、コンフェデレーション内の AS をコンフェデレーション内に存在しない AS と区別します。リモート AS の観点では、コンフェデレーション ID は AS ID です。リモート AS は、一意の AS ID をもつ複数のサブ AS であることを知りません。

サブ AS に対する任意の有効な AS 番号を使用できます。もし AS がインターネットへ接続されている場合、プライベート AS の範囲(64512 - 65535)内の数字を使用することをプロケードは推奨します。これらは、プライベート AS の数値で、BGP4 ルータはインターネットへ、これらの AS 番号を広告しません。

ネクスト・ホップ・セルフ(Next-Hop-Self)

BGP コマンド `neighbor x.x.x.x next-hop-self` は、IBGP ネイバに適用されます。next-hop-self は、プロトコルが選択したネクスト・ホップよりもむしろ、特定のネイバへ送信された経路更新において自分自身をネクスト・ホップとして指定します。このオプションは、デフォルトでは無効です。

BGP テーブル

各 BGP ルータは BGP テーブルをもっています。BGP テーブルは、宛先ネットワーク、ネクスト・ホップ、MED (Multi-Exit Discriminator, metric)、ローカル優先度(Local Preference)、ウエイト及び AS パスなどの属性情報を含みます。”>” は、宛先ネットワークへ到達するベスト・パスのルートを示しているため、ルーティング・テーブルにのっています。

以下は、出力例です:

```
Total number of BGP Routes: 14
Status codes: s suppressed, d damped, h history, *valid, >best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
*>i 161.19.7.192/26 161.19.7.5 0 100 25 100 11 i
* 161.19.7.192/26 161.19.8.5 50 200 0 100 100 11 i
*>i 161.49.4.0/26 161.49.5.2 0 300 25 10 i
*>i 161.49.4.64/26 161.49.5.2 0 300 25 10 i
*>i 161.49.4.128/26 161.49.5.2 0 300 25 10 i
*>i 161.49.4.192/26 161.49.5.2 0 300 25 10 i
*> 161.49.6.0/24 0.0.0.0 50 200 32768 i
*i 161.49.6.0/24 161.49.7.1 0 100 25 i
```

コマンド show ip bgp routeは、類似の情報を示しています:

```
FastIron#show ip bgp route
Total number of BGP Routes: 5
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED H:HISTORY
I:IBGP L:LOCAL M:MULTIPATH S:SUPPRESSED
Prefix      Next Hop      Metric      LocPrf      WeightStatus
1 0.0.0.0/0    10.1.0.2      0           100 0        BI AS_PATH: 65001 4355 701 80
2 102.0.0.0/24 10.0.0.1      1           100 0        BI AS_PATH: 65001 4355 1
3 104.0.0.0/24 10.1.0.2      0           100 0        BI AS_PATH: 65001 4355 701 1 189
4 240.0.0.0/24 102.0.0.1     1           100 0        BI
AS_PATH: 65001 4355 3356 7170 1455
5 250.0.0.0/24 209.157.24.11 100 0        I AS_PATH: 65001 4355 701
```

ルーティング・テーブル

各ルータは各宛先ネットワークに対するベスト・ルートを含むルーティング・テーブルをもっています。以下に例を示します:

```
FastIron#show ip route
Total number of IP routes: 50834
B:BGP D:Directly-Connected O:OSPF R:RIP S:Static
Network Address NetMask Gateway Port Cost Type
3.0.0.0 255.0.0.0 192.168.13.21/1 0 B
4.0.0.0 255.0.0.0 192.168.13.21/1 0 S
9.20.0.0 255.255.128.0 192.168.13.21/1 0 B
10.1.0.0 255.255.0.0 0.0.0.0 1/1 1 D
10.10.11.0 255.255.255.0 0.0.0.0 2/24 1 D
12.2.97.0 255.255.255.0 192.168.13.21/1 0 O
```

Type の縦の欄は、ネットワークをどのプロトコルから学習したかを示しています。

AS パス

BGP の基本概念は、AS パスをまたがる自律システム(AS)を各 BGP パケットが追跡するという考えです。もしあるルータが自分の AS 番号を AS パス内に検知すると、ループと判断しパケットをドロップします。

BGP 属性 - 属性は、たとえば AS パス情報及びルート起源(route origin)のようにルートに固有の情報を追跡します。属性は、ベスト・ルートをフィルタリングし、選択するのに使用されます。ネクスト・ホップ及び AS パスは属性の例です。

ルーティング・ループ - もっとも重要な BGP への追加は、AS パスを確認することによって、もしパケットが入ってきたときに、同じ AS を含んだパケットを受信する場合、パケットをドロップし、ルーティング・ループを防止する能力です。

そのルートの AS パスの先頭にローカル AS 番号を追加できます。AS パスの長さに基づいて他のルートと比較したとき、その AS パスに AS 番号を追加すると、そのルートがより選択されなくなります。

BGP ネイバとルート情報の概要を表示する便利なコマンド

```
show ip bgp summary show ip bgp config
show ip bgp neighbor
show ip bgp neighbor x.x.x.x
show ip bgp neighbor x.x.x.x routes-summary
show ip bgp neighbor x.x.x.x advertised-routes
show ip bgp
show ip bgp route
show ip bgp route summary
show ip bgp route best
show ip bgp route unreachable
show ip bgp flap-statistics
```

5- アドバンスド・レイヤ3 の概念

デフォルト・ルートの生成

プロケードのデバイスが OSPF 自律境界ルータ(ASBR)の場合、外部のデフォルト・ルートを OSPF ルーティング・ドメインに自動的に生成するよう設定できます。この機能は、“デフォルト・ルート生成”、または“デフォルト情報の生成”と言われます。

デフォルトでは、プロケードのデバイスは OSPFv3 ドメインにデフォルト・ルートを広告しません。OSPF のデフォルト・ルートを広告したい場合、デフォルト・ルートの生成(default route origination)を明示的に有効にしなければなりません。

OSPF のデフォルト・ルート生成を有効にすると、デバイスはスタブ・エリア以外のすべての AS にフラッドされるタイプ 5 のデフォルト・ルートを広告します。OSPF ルートの再配布が有効でなくても、また、デフォルト・ルートが IBGP ネイバ経由で学習していなくても、デバイスはデフォルト・ルートを OSPF に広告します。明示的にデフォルト・ルートの生成を有効にしない限り、その他の設定パラメータがあっても、OSPF のデフォルト・ルートを広告しないことに注意してください。

たとえば、メトリック 2 及びタイプ 1 の外部ルートをもつデフォルト・ルートを広告するためには、次のコマンドを入力してください:

```
FastIron(config-ospf6-router)#default-information-originate always metric 2 metric-type type1
```

Syntax: [no] default-information-originate [always] [metric <value>] [metric-type <type>]

`always` keyword キーワードは、デバイスがデフォルト・ルートを学習しているかどうかにかかわらず、デフォルト・ルートを生成します。このオプションは、デフォルトでは無効です。

メトリック<値>パラメータはデフォルト・ルートに対するメトリックを指定します。このオプションが使用されない場合、`default-metric` コマンドの値がそのルートに対して使用されます。`metric-type<値>`パラメータは OSPF ルーティング・ドメインに広告されたデフォルト・ルートに関係した外部リンクのタイプを指定します。その<タイプ>は次のいずれかになります:

- タイプ 1 外部ルート
- タイプ 2 外部ルート

もしこのオプションを使用しない場合、デフォルト再配布のメトリック・タイプがそのルート・タイプに対して使用されます。

IP ルートの選択及び管理ディスタンス

IP ルータはルックアップのメカニズムを使用します。ルーティング・テーブル内の最長プレフィックスにマッチしたアドレスをもつ各入力パケットのネクスト・ホップを検索するために IP ルックアップは重要なルータのアクションです。つまり、ルータが宛先へのパスを決定するとき、最長プレフィックスにマッチしたエントリを最初に選択します。

同じ宛先ネットワークに対して異なる送信元から学習した複数のエントリがあるかもしれませんが、これらのエントリは同じプレフィックス長を持っている場合があります。これらの異なる送信元は、BGP4、OSPF、RIP、スタティック・ルートなどかもしれません。ソフトウェアは、各ルートの管理ディスタンスに基づいてそのルートを比較します。

もしそのパスの管理ディスタンスが他のソース(たとえば、スタティック IP ルート、RIP または OSPF)からのパスの管理ディスタンスより低い場合、BGP4 のパスが IP ルート・テーブルにインストールされます。

以下にプロトコド・ルータのデフォルトの管理ディスタンスを示します:

- 直結(Directly connected) - 0 (この値は設定できません)
- スタティック - 1 (デフォルト・ルートを含むすべてのスタティック・ルートに適用されます)
- EBGp - 20
- OSPF - 110
- RIP - 120
- IBGP - 200
- Local BGP - 200
- 不明(Unknown) - 255 (ルータはこのルートを使用しません)

より低い値の管理ディスタンスが優先されます。もしルータが OSPF 及び RIP から同じネットワークのルートを受信する場合、ルータはデフォルトで OSPF のルートを優先します。

ルートの再配布

再配布は、複数のルーティング・プロトコルが動作しているルータ上で実行されます。たとえば OSPF 及び RIP という複数のルーティング・ドメインの境界をなすボーダ・ルータで動作します。RIP 及びスタティック・ルートで学習した経路を OSPF に再配布する例を以下に示します:

```
FastIron(config)#router ospf
FastIron(config-ospf-router)#redistribution rip
FastIron(config-ospf-router)#redistribution static
```

再配布のフィルタを設定するまで再配布を有効にしないでください。そうしないと、意図せず、再配布を必要としないルートでネットワークに負荷をかけ過ぎる可能性があります。

IPv6

IPv6 アドレスは、128 ビット長のアドレスを 16 ビットごとに 16 進数の値で、コンマ(:)によって区切られた 8 フィールドで構成されます:

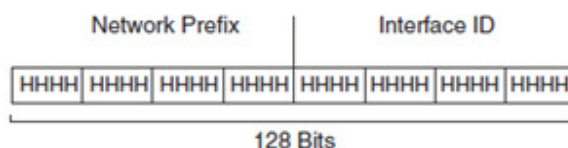


図 3: IPv6 アドレス・フォーマット

HHHH は、16 ビットの 16 進数の値(0000 から FFFF まで)です。H は、4 ビットの 16 進数の値になります。

次は、IPv6 アドレス: 2001:0000:0000:0200:002D:D0FF:FE48:4672 の例です。

IPv6 アドレスがゼロの 16 進数のフィールドを含むことに注意してください。長くてわかりにくならないように、次のように記述できます:

- フィールド上のゼロを省略できます; 例) 2001:0:0:200:2D:D0FF:FE48:4672
- IPv6 アドレスの最初、中間、最後など場所を問わず、連続したゼロのフィールドをアドレス毎に 1 回の 2 つのコロン(::) に要約できます; 例) 2001::200:2D:D0FF:FE48:4672
- コマンド構文において IPv6 アドレスを指定するとき、最も長く連続した 16 進数のゼロのフィールドを表現するために、アドレス内で 1 回のみ 2 つのコロン (::) を使用できます; 例) 2001:0:0:0:2D:0:0:4672 -> 2001::2D:0:0:4672
- IPv6 アドレスの 16 進数の文字は大文字と小文字を識別しません

IPv6 アドレスのタイプ

- ユニキャスト(Unicast): 単一インタフェイスに対するアドレス。ユニキャスト・アドレスに送信されたパケットは、アドレスによって明確にされたインタフェイスへ送られます。ユニキャスト・アドレスには、集約可能なグローバル・アドレス(プレフィックス 2000::/3)、サイト・ローカル・アドレス(プレフィックス FEC0::/10)、リンク・ローカル・アドレス(プレフィックス FE80::/10)、IPv4 互換アドレス(0:0:0:0:0:A.B.C.D)、ループバック・アドレス(0:0:0:0:0:0:0:1 または ::1)、未特定アドレス(0:0:0:0:0:0:0:0 または ::)などいくつかのタイプがあります。
- マルチキャスト(Multicast): 異なるノードに所属するインタフェイス・セットのアドレス。マルチキャスト・アドレスにパケットを送信することによって、すべてのインタフェイスへまとめて送られます。マルチキャスト・アドレスは固定のプレフィックス FF00::/8 (1111 1111)をもっています。次の 4 ビットは、既知または一時的アドレスとして定義します。その次の 4 ビットはアドレスのスコープ(ノード、リンク、サブネット、アドミン、サイト、組織、グローバル)を定義します。
- エニーキャスト(Anycast): 異なるノードに属するインタフェイス・セットに対するアドレス。パケットをエニーキャスト・アドレスに送信することによって、アドレスによって明確にされた最も近いインタフェイスにパケットを送ります。

PIM Sparse モード(PIM-SM)

プロケードのデバイスは Protocol Independent Multicast (PIM) Sparse バージョン 2 をサポートします。PIM Sparse は、広範囲に配信するマルチキャスト環境に適したマルチキャストリングを提供します。PIM Sparse ネットワークにおいて、マルチキャスト・グループに対する情報を受信したいホストに接続された PIM Sparse ルータは、受信ホストにかわって参加要求(join request)を明示的に送信しなければなりません。

PIM Sparse ルータは、ドメインで構成されます。PIM Sparse ドメインは、すべてが PIM を実装したルータの連続したセットで、共通の境界内で動作するように構成されます。

IGMP スヌーピングの概要

デバイスがマルチキャストのパケットを処理するとき、デフォルトでは VLAN の入力ポート以外のすべてのポートにパケットをブロードキャストします。パケットは、CPU を介さずにハードウェアによってフラッディングされます。この動作によっていくつかのクライアントは、不必要なトラフィックを受信します。IGMP スヌーピングは特定のマルチキャスト・グループ(宛先アドレス)に対する IGMP レシーバをもつポートにのみトラフィックを転送することによってマルチキャストを抑制します。デバイスは、IGMP レポート及びリーブ・メッセージを処理することによって、IGMP グループのメンバシップ情報を維持します。それによってトラフィックは IGMP レポートを受信するポートに転送されます。

ポートからトラフィックを削除する前に、ポート上のどのクライアントも特定のトラフィックを必要としないことを確認するために IGMP デバイスは責任をもって、定期的により一般クエリをブロードキャストし、また、リーブ・メッセージを受信するとグループ・クエリを送信します。

IGMP スヌーピングは、マルチキャストのフローが VLAN のすべてのスイッチ・ポートにフラッディングされるのを防止するレイヤ 2 のメカニズムです。スイッチはルータ及びホスト間の通信をスヌーピング(聞くこと)することで VLAN 内のレイヤ 3 IGMP パケットを調査します。スイッチはどのポートがシグナリングするか、またはどのポートがマルチキャスト・グループをリーブするかをレイヤ 3 で学習します。スイッチはどのインタフェイスが、このトラフィックの受信に関心があるホストに接続されているかを検知します。スイッチは、IGMP メッセージ・タイプに基づき、レイヤ 2 マルチキャスト転送グループにポートを追加またはそのグループから削除します。マルチキャスト・ストリームはフローを明示的に要求するポートに送信されます。IGMP スヌーピングはすべての VLAN へのフラッディングを回避することによって帯域の消費を削減します。IGMP スヌーピング機能は、どのポートがマルチキャスト対応ルータに接続しているかをトラックして、IGMP メンバシップ・レポートの転送管理を支援します。

VRRP 及び VRRP-E の比較

ほとんどのパラメータ及びデフォルト値は VRRP 及び VRRP-E 双方に対して同じです。いくつかの異なる点を以下に示します:

- プロトコル: RFC2338 にて定義された仮想ルータ冗長プロトコル - Virtual Router Redundancy Protocol (VRRP) または VRRP-Extended(プロケードが拡張実装した VRRP)
- 仮想ルータ ID(VRID): ゲートウェイとなる IP インタフェイスをバックアップする複数のルータを設定することによって作成する仮想ルータの ID。アドレスをバックアップするために使用したい各ルータ上で同じ VRID を設定しなければなりません。
- 仮想ルータの IP アドレス: これは、バックアップするアドレスです。
 - VRRP - 仮想ルータ IP アドレスはいずれかひとつの VRRP ルータの VRID インタフェイスで設定された実 IP アドレスでなければなりません。このルータは、IP アドレスのオーナーでデフォルトではマスタです。この VIP アドレスはホストから到達可能です。もしオーナーが障害で、バックアップ・ルータが新しいマスタになる場合、VIP はホストから PING で到達性をもちません。
 - VRRP-E - 仮想ルータ IP アドレスは、VRRP-E インタフェイスで設定された実 IP アドレスと同じサブネットでなければなりません。しかし、インタフェイスで設定された実 IP アドレスと同じにはできません。
- VRID MAC アドレス: VRID インタフェイスから送信された VRRP または VRRP-E 内のパケット送信元 MAC アドレス及び VRID へ送信されたパケットに対する宛先 MAC アドレス:
 - VRRP - 00-00-5e-00-01-<vrid>として定義された仮想 MAC アドレス。マスタは仮想 MAC アドレスを所有しています。
 - VRRP-E - 02-E0-52-<ハッシュ値>-<vrid>として定義された仮想 MAC アドレス。<ハッシュ値>は、IP アドレスに対する 2 オクテットのハッシュ化した値です。<vrid>は、VRID です。
- 認証のタイプ: VRRP または VRRP-E ルータが VRRP または VRRP-E パケットを証明するために使用する認証のタイプ。OSPF のようなルーティング・プロトコルで使用されるような VRID ポート同士が使用する認証タイプに一致しなければなりません:
 - 認証なし - インタフェイスは、認証を使用しません。これは、VRRP のデフォルトです。
 - シンプル - インタフェイスはインタフェイス上に送信されるパケットのパスワードとして、シンプルなテキスト・ストリングを使用します。インタフェイスがシンプルなパスワード認証を使用する場合、インタフェイス上の VRID 設定は、同じ認証タイプと同じパスワードを使用しなければなりません。
 - MD5 は、VRRP または VRRP-E ではサポートしていないことに注意してください。
- ルータのタイプ: ルータはオーナーまたはバックアップのいずれかになります。
 - オーナー(VRRP のみ) - VRID によって使用される実 IP アドレスが設定されるルータ。オーナーは常に、VRID によって使用される実 IP アドレスをもつルータです。VRID に対するすべての他のルータはバックアップになります。

- バックアップ - VRID に対するルーティングサービスを提供するルータで、VRID に一致する実 IP アドレスをもたないルータ。VRRP-E では、VRID に対するすべてのルータはバックアップです。
- バックアップ優先度: VRID に対してマスタになるためのバックアップ優先度を決定する数値。ネゴシエーションの間、最も高い優先度をもつルータがマスタになります。
 - VRRP - オーナは最も高い優先度(255)をもちます。他のルータは、3 から 254 の間の優先度をもつことができます。デフォルト値は、オーナが 255 で各バックアップは 100 です。
 - VRRP-E - すべてのルータは、バックアップでデフォルトでは同じ優先度をもちます。デフォルト値はすべてのバックアップで 100 です。
 - 2つ以上のバックアップが同じ最も高い優先度を持つ場合、最も高い IP アドレスをもつバックアップのインタフェイスがその VRID に対してマスタになります。
- トラック・ポート: レイヤ 3 スイッチの別のポートまたは VRID インタフェイスによってリンク状態がトラックされる仮想インタフェイス。もしトラックされたインタフェイスに対するリンクがダウンすると、VRID インタフェイスの VRRP または VRRP-E 優先度が変化して、マスタに対するネゴシエーションが再度、発生します。
- トラック優先度: トラックされたポートに割り当てられた VRRP または VRRP-E 優先度の値。トラックされたポートのリンクがダウンする場合、VRID ポートの VRRP または VRRP-E 優先度が変化します。
 - VRRP - 優先度はトラックされたポートの優先度の値に変化します。その値は、デフォルトで 2 になります。
 - VRRP-E - VRID ポートの優先度は、トラックされたポートの優先度の合計分、削減されます。その値は、デフォルトで 5 になります。
- バックアップ・プリエンプト・モード: より高い VRRP 優先度をもつバックアップがより低い優先度をもちながら、すでに VRID の制御を引き受けていた別のバックアップから VRID の制御を奪うことを防止します。このモードは、デフォルトで有効です。
- VRRP-E スロー・スタート・タイマ: この機能は、マスタが復旧する時間及びバックアップからマスタを引き継いだ時間の間、特定の待ち時間を生成します。この間隔は、マスタが復旧するとき OSPF の収束の時間を与えます。デフォルトは、無効になっています。

レイヤ 2 及びレイヤ 3 のマルチキャスト・アドレス・マッピング

マルチキャスト・アドレスの 01-00-5E-00-00-00 から 01-00-5E-7F-FF-FF までの範囲は、IP マルチキャストリングのために予約されています。下図で示しているとおり、48 ビット MAC アドレスの上位 25 ビットは固定で、下位 3 ビットは可変です。

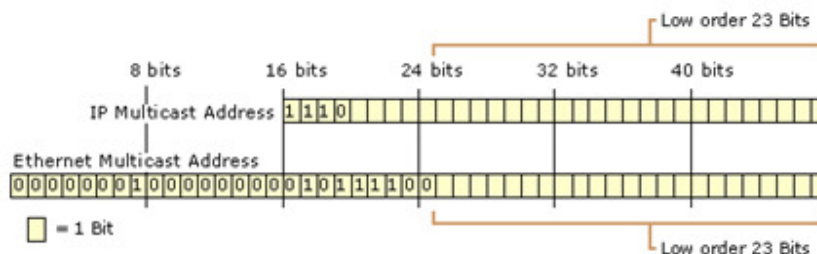


図 4: マルチキャスト・アドレスのレイアウト

レイヤ 3 の IP マルチキャスト・アドレスをレイヤ 2 の MAC マルチキャスト・アドレスにマッピングするために、IP マルチキャスト・アドレスの下位 23 ビットが MAC マルチキャスト・アドレスの下位 23 ビットと直接マッピングされます。クラス D の規定では、IP マルチキャスト・アドレスの先頭から 4 ビットは固定です。MAC マルチキャスト・アドレスにマッピングしていない IP マルチキャスト・アドレスが 5 ビット分あるため、ホストが属していないグループの MAC マルチキャスト・ダイアグラムを受信する可能性があります。これらのパケットは宛先 IP アドレスが決定されるとレイヤによってドロップされます。

たとえば、マルチキャスト・アドレス 239.192.16.1 は、01-00-5E-40-10-01 になります。下位 23 ビットを使用すると、先頭のオクテットは使用されず、2 つ目のオクテットの後ろから 7 ビットのみが使用されます。3 番目と 4 番目のオクテットは 16 進数に直接変換されます。2 番目のオクテット、192 は 2 進数で 11000000 になります。上位ビットを取り除くと、1000000、または 64 (10 進数表記)、または 0x40 (16 進数表記) になります。次のオクテット 16 は 16 進数で 0x10 になります。最後のオクテット 1 は、16 進数で 0x01 になります。したがって 239.192.16.1 に相当する MAC アドレスは、01-00-5E-40-10-01 になります。

PBR

ポリシー・ベースのルーティング(PBR)によって ACL 及びルートマップを使用し、IP パケットを選り分け、変更してハードウェアでのルーティングをすることができます。ACL はトラフィックをクラス分けします。ACL に一致したルートマップで、トラフィックに対するルーティング属性を設定します。PBR ポリシはポリシーに一致したトラフィックに対してネクスト・ホップを指定します。PBR をもつ標準 ACL を使用すると、送信元 IP アドレスに基づいたルーティングができるようになります。拡張 ACL をもつ ACL を使用すると、拡張 ACL 内に記載したすべての文節に基づいた IP パケットをルーティングできるようになります。

以下に示すレイヤ 3 及びレイヤ 4 情報に基づいた PBR のタイプを設定できます:

- ネクストホップ・ゲートウェイの選択
- ヌル・インタフェイス(null0)へのパケットの送信

ポリシーが複数のネクスト・ホップをもつ場合、PBR は稼働中のポリシー内で指定した初めのネクスト・ホップを選択します。もし、どのポリシーのダイレクト・ルートまたはネクスト・ホップも利用できない場合、パケットは通常通り、ルーティングされます。

6 - レイヤ2 プロトコル

MRP

MRP (メトロ・リング・プロトコル)は、レイヤ 2 ループを防止し、レイヤ 2 リング・トポロジ内の高速な収束を提供するブロード独自のプロトコルです。STP に代わる、特にメトロ・エリア・ネットワーク(MAN)に有効なプロトコルです。以下に、MRP メトロ・リングの例を示します(F: フォワーディング, B: ブロックング)。

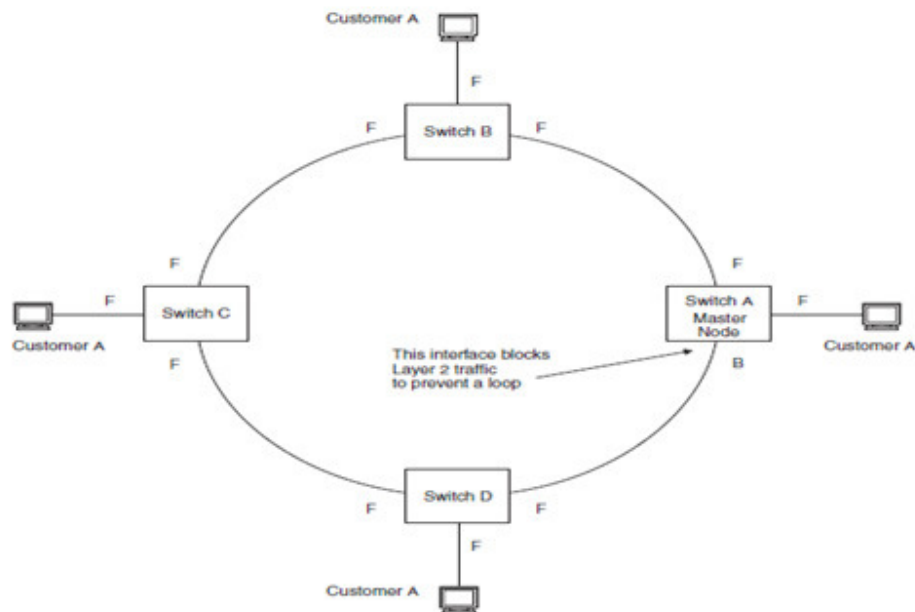


図 5: メトロ・リングの例

この例のリングは、4 つの MRP ノード(ブロードのスイッチ)から構成されています。各ノードは 2 つのリングのインタフェイスをもっています。各ノードはまた、別の顧客ネットワークへ接続されます。ノードはリングを経由して顧客ネットワークを往来するレイヤ 2 トラフィックをフォワードします。リングのインタフェイスはひとつのポート・ベース VLAN にすべて含まれます。各顧客のインタフェイスは、同じ VLAN または個別の VLAN にリングとして収容できます。

1 ノードは、MRP リングのマスタ・ノードとして設定できます。マスタ・ノード上の 2 つのインタフェイスのうちいずれか 1 つはプライマリ・インタフェイスとして設定できます。もう 1 つはセカンダリ・インタフェイスになります。プライマリ・インタフェイスは、リングのヘルス・パケット(RHP)を生成し、リングの健全性を監視するために使用されます。RHP がマスタ・ノードのセカンダリ・インタフェイスに到達するまで、RHP はリング上で次のインタフェイスへ転送されます。セカンダリ・インタフェイスはレイヤ 2 ループを防止するためにパケットをブロックします。MRP は、was introduced in two phases: MRP フェーズ 1 及びフェーズ 2 という 2 段階で導入されました。

シェアード・インタフェイスをもたない MRP リング(MRP フェーズ 1):

MRP フェーズ 1 は、下記の図のとおり、複数の MRP リングを構成できますが、リングは同じリンクを共有できません。たとえば、リング 1 及びリング 2 がそれぞれインタフェイス 1/1 及びインタフェイス 1/2 をもつように構成することができません。また、MRP リングを構成するとき、リング上の任意のノードがリングに対するマスタ・ノードとして設計できます。

マスタ・ノードは複数のリングのマスタ・ノードになれます。各リングは、独立したリングで、RHP パケットは各リング内で処理されます。

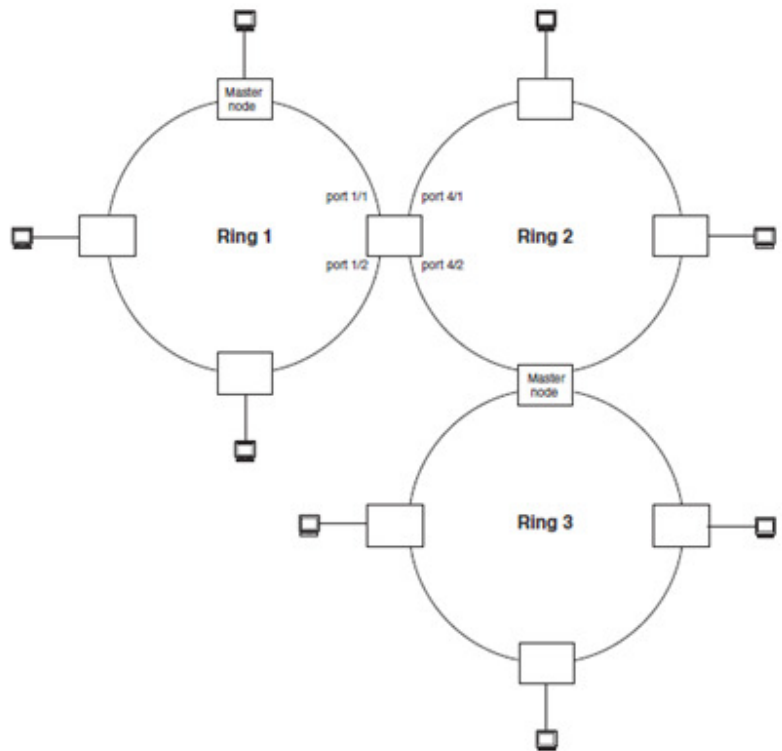


図 6: 複数のメトロ・リング

上記の図では、2つのノードがそれぞれ2つのMRPリングをもって構成されています。リングのどのノードもそのリングに対するマスタになれます。ノードはまた、複数のリングに対するマスタになれます。

MRP フェーズ 1 は、以下の MRP 状態のいずれかになります:

- プリフォワーディング(PF) - インタフェイスは RHP を転送できますが、データは転送できません。すべてのリングのポートは、MRP を有効にすると、この状態で始まります。
- フォワーディング(F) - インタフェイスは RHP と同様にデータも転送できます。ポートのプリフォワーディングがタイムアウトすると、インタフェイスはプリフォワーディングからフォワーディングへ変化します。タイムアウトは、ポートがマスタから RHP を受信しない場合、またはポートが受信した RHP 内のフォワーディング・ビットがオフの場合に生じます。これはリングが途切れていることを示します。そのポートは状態をフォワーディングへ変化させることでリングを復旧させます。プリフォワーディング時間は、RHP を受信しなくても、フォワーディング状態に変化する前にプリフォワーディング状態でポートが保持するミリ秒単位の数値です。
- ブロッキング(B) - インタフェイスはデータを転送できません。マスタ・ノード上のセカンダリ・インタフェイスだけがブロッキングになります。

MRP が有効な場合、すべてのポートはプリフォワーディング状態で始まります。マスタ・ノード上のプライマリ・インタフェイスは、他のポートと同様にプリフォワーディング状態ですが、すぐにリング上へ RHP を送信します。マスタ・ノード上のセカンダリ・ポートは、RHP に対して傾聴します。

- セカンダリ・ポートが RHP を受信すると、リングのすべてのリンクがアップし、ポートはブロッキング状態に遷移します。プライマリ・ポートは、フォワーディング・ビットをオンにして別の MRP を送信します。各メンバ・ポートが RHP を受信すると、ポートはフォワーディング状態に遷移します。一般的に、これは、一秒以内に生じます。リングはすぐに完全に初期化された状態になります。
- セカンダリ・ポートはプリフォワーディング時間が満了するまでに RHP を受信しない場合、リングの切断が生じます。そのポートはフォワーディング状態に遷移します。メンバ・ポートはまた、プリフォワーディング時間が満了するとプリフォワーディングからフォワーディングへ遷移します。リングは完全な状態ではないですが、データはアップしているリンクを使用してノード間で運ばれます。

シェアード・インタフェイスをもつ MRP リング (MRP フェーズ 2):

MRP リングは、インタフェイスが同じ VLAN に属する条件で、同じインタフェイスを共有するように構成できます。以下の図でいくつかの例を示します:

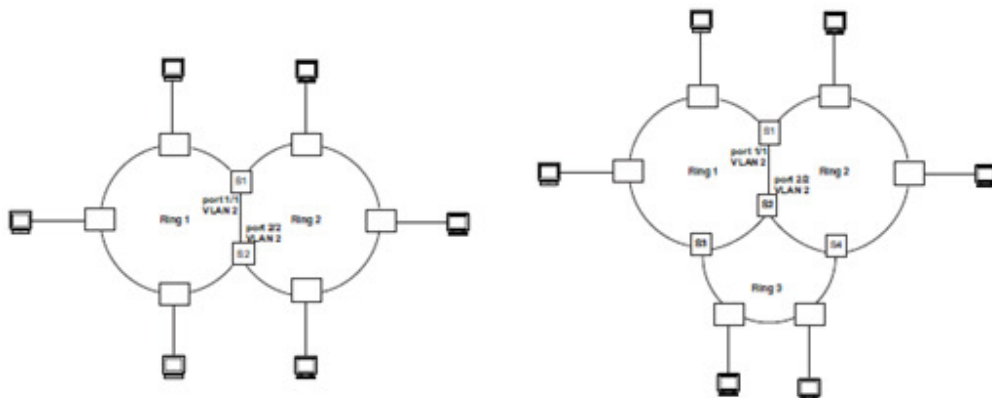


図 7: インタフェイスを共有している複数の MRP リング

上記の 2 つの図は同じインタフェイスを共有する複数の MRP リングの例を示しています (Phase 2)。

リング情報を表示するためには、以下のコマンドを入力します:

```
FastIron#show metro
Metro Ring 1
=====
Ring State      Ring      Master Topo      Hello      Prefwing
id             role      vlan  group      time (ms)   time (ms)
2      enabled  member      2      not conf    100         300

Ring interfaces Interface role Forwarding state Active interface Interface Type
ethernet 1/1   primary   disabled      none        ethernet 2     Regular
ethernet 1/2   secondary forwarding     ethernet 2     Tunnel

RHPs sent      RHPs rcvd      TC RHPs rcvd      State changes
3              0              0                 4
```

RSTP ブリッジ及びブリッジ・ポートの役割

IEEE 802.1W 機能は、ブリッジまたはブリッジ・ポートの障害後、数ミリ秒(0 から 500 ミリ秒)でポイント・ツー・ポイントのリンクに対する高速なトラフィックの収束を提供します。この収束は、802.1D STP または RSTP ドラフト 3 によって提供される収束より速く発生します。

802.1W の高速なスパニング・ツリーのトポロジ内のブリッジが、トポロジで最も高いプライオリティ(最も低いブリッジ識別子)の場合、ルート・ブリッジとして割り当てられます。他のブリッジは非ルート・ブリッジになります。独自の役割がルート・ブリッジ及び非ルート・ブリッジ上のポートに割り当てられます。RST BPDU 内に含まれる以下の情報に基づいて役割が割り当てられます:

- ルート・ブリッジ ID (Root bridge ID)
- パス・コスト値 (Path cost value)
- 送信ブリッジ ID (Transmitting bridge ID)
- 代表ポート ID (Designated port ID)

ポートが受信する RST BPDU はポートが送信する RST BPDU より優先されるかどうかを決定するために、802.1W アルゴリズムは、この情報を使用します。2つの値は、上述のルート・ブリッジ ID から昇順で比較されます。低い値をもつ RST BPDU が優先されます。RST BPDU の優劣はポートへの役割を割り当てるために使用されます。

受信した RST BPDU の値が送信した RST BPDU の値と同じ場合、RST BPDU 内のポート ID が比較されます。より低いポート ID をもつ RST BPDU が優先されます。その後、ポートの役割が、適切に計算されます。ポートの役割は、ポートが送信する BPDU 内に含まれます。802.1W のポートによって送信された BPDU は、RST BPDU としてみなされ、802.1W モードで動作します。

ポートは、次のいずれかの役割をもちます:

- ルート(Root) – 特定のブリッジからルート・ブリッジまでの最も低いパス・コスト値を提供します。
- 代表(Designated) – 接続されている LAN からルート・ブリッジへの最も低いコスト値を提供します。
- 代替(Alternate) – ルート・ポートがダウンした場合、ルート・ブリッジへの代替パスを提供します。
- バックアップ (Backup) – 代表ポートがダウンした場合、LAN へのバックアップを提供します。
- 無効(Disabled) – トポロジ内での役割をもちません。

ポートの役割の割り当て: システム起動時に、すべての 802.1W が有効なブリッジ・ポートは代表の役割をもちます。起動が完了すると、802.1W アルゴリズムがポートで送受信した RST BPDU の優劣を計算します。

ルート・ブリッジ上では、物理的に同時に 2 本接続された同一ブリッジ上のポートを除いて、各ポートは代表ポートの役割を割り当てられます。これらのタイプのポートで、優先度の高い RST BPDU を受信するポートはバックアップ・ポートになります。一方、他のポートは代表ポートになります。

非ルート・ブリッジ上で、ポートは次のとおりに割り当てられます:

- ルート・ブリッジからリンク帯域幅に基づく最も低いパス・コストをもつ RST BPDU を受信するポートは、ルート・ポートになります。
- 同一ブリッジ上に 2 ポートが物理的に接続されている場合、優先度の高い RST BPDU を受信するポートはバックアップ・ポートになります。一方、他のポートは代表ポートになります。
- 非ルート・ブリッジがすでにルート・ポートをもつ場合、送信する RST BPDU より優先度の高い RST BPDU を受信するポートは代替ポートになります。
- ポートが受信する RST BPDU が送信する RST BPDU より優先度が低い場合、そのポートは代表ポートになります。
- ポートがダウンした場合、または 802.1W がポートで無効な場合、そのポートは無効ポートの役割が与えられます。無効ポートはトポロジ内で役割をもちません。しかし、802.1W がリンク・ダウンしたポートで有効な場合で、そのポートのリンクがアップした場合、そのポートは次のいずれかのポートの役割をもちます: ルート、代表、代替、無効

最も低いブリッジ ID(ブリッジ優先度+MAC アドレス)をもつスイッチは、ルート・ブリッジになります。ルート・ブリッジ上のすべてのポートは転送状態になります。それぞれの非ルート・ブリッジはどのポートが転送すべきか、ブロックすべきかを決定するために以下に示す基準を使用します:

1. ルート・ブリッジへのすべてのパス・コスト
2. 最も低い送信元のブリッジ ID
3. 最も低い送信元のポート ID (ポート優先度+ポート番号)

802.1W の要約を表示するには、次のコマンドを使用してください: `show 802-1w [vlan <vlan-id>]`

```
FastIron#show 802-1w
--- VLAN 1 [ STP Instance owned by VLAN 1 ] -----
VLAN 1 BPDU cam_index is 2 and the IGC and DMA master Are (HEX) 0 1 2 3

Bridge IEEE 802.1W Parameters:
Bridge          Bridge          Bridge Bridge          Force          tx
Identifier      MaxAge          Hello FwdDly          Version        Hold
hex             sec      sec      sec                  cnt
800000e080541700 20      2      15                  Default        3

RootBridgeID    RootPathCost  Designated_BridgeID    Root_Port    MaxAge FwdDly
Hello
hex             hex             sec                  sec          sec
800000e0804c9c00 200000          800000e0804c9c00 1              20      15      2

Port IEEE 802.1W Parameters:
<--- Config Params ----->|<----- Current state ----->|
Port Pri PortPathCost P2P MAC Edge Port Role State Desig. Cost Desig. bridge
1  128  200000          F  F  ROOT FORWARDING 0
800000e0804c9c00
2  128  200000          F  F  ALTERNATE DISCARDING 200000
800000e080548400
3  128  200000          F  F  DESIGNATED FORWARDING 200000
800000e080541700
4  128  200000          F  F  BACKUPDISCARDING 200000
800000e080541700
```

DHCP スヌーピング

動的ホスト構成プロトコル(DHCP)スヌーピングは、サブネット内の信頼されていない DHCP パケットをフィルタリングします。DHCP スヌーピングは、たとえば、誤って他のユーザに教えるつもりで DHCP 応答パケットを送信してしまったりすることや、DHCP サーバのふりをする悪意のあるユーザのような中間者攻撃(man-in-the-middle attack)などを防止することができます。DHCP スヌーピングはまた、認可されていない DHCP サーバを停止させ、ユーザの DHCP サーバの設定ミスによるエラーを防止できます。DHCP スヌーピングは、動的 ARP 検査(Dynamic ARP Inspection)及び IP ソース・ガード(IP Source Guard)と一緒によく使用されます。

DHCP スヌーピングの動作

VLAN 上で DHCP スヌーピングが有効な場合、DHCP スヌーピングは untrusted ポート(ホストが接続されたポート)及び trusted ポート(DHCP サーバが接続されたポート)間で動作します。DHCP スヌーピングが有効な VLAN は、DHCP リクエスト・パケットをクライアントから転送し、untrusted ポート上の DHCP サーバのリプライ・パケットを破棄し、trusted ポートの DHCP クライアントへ DHCP サーバのリプライ・パケットを転送します。

スパニング・ツリー・プロトコル (STP)

STP は、ブリッジ及び設定できるポート・パラメータに基づいて、あるポートをブロックし、他のポートでトラフィックを転送する選択をすることでネットワーク上のレイヤ 2 ループを排除します。プロセードのレイヤ 2 及びレイヤ 3 スイッチは、IEEE 802.1D の仕様に記載された標準の STP をサポートします。STP は、レイヤ 2 スイッチでは、デフォルトで有効ですが、レイヤ 3 スイッチでは、デフォルトで無効です。デフォルトでは、プロセードのデバイスの各ポート VLAN で、個別のスパニング・ツリー(個別の STP インスタンス)が動作しています。プロセードのデバイスは、デフォルトですべてのデバイス・ポートを含むポート・ベース VLAN(VLAN 1)をもっています。このように、デフォルトでは、各プロセードのデバイスは、ひとつのスパニング・ツリーをもつこととなります。しかしながら、追加でポート・ベース VLAN をプロセードのデバイス上で設定すると、STP が有効な各 VLAN 及び VLAN 1 では、すべて個別のスパニング・ツリーが動作します。

PVST では、VLAN 毎にスパニング・ツリー・インスタンスをもっています。各 VLAN がそれぞれルート・ブリッジをもっています。ひとつの STP インスタンスによってブロックされたポートは、ユーザ・トラフィックを転送するために別の STP インスタンスによって使用されるので、ロードバランスが実現できます。

デフォルトでは、プロセードのデバイス上の各ポート・ベースで、個別のスパニング・ツリーが動作し、個々の VLAN 単位で有効化または無効化できます。別の手法として、デバイスのすべてのポート及び VLAN でシングル・スパニング・ツリーをプロセードのデバイスに設定できます。シングル STP (SSTP)機能は、802.1Q 仕様に準じたシングル・スパニング・ツリーを動作させるサード・パーティのデバイスにプロセードのデバイスを接続することに対して特に役に立ちます。

802.1W RSTP は、ブリッジまたはブリッジ・ポートの障害後、ポイント・ツー・ポイントのリンクに対して数百ミリ秒(0-500 ミリ秒)以内の高速なトラフィックの収束を提供します。この収束は、802.1D STP による収束より、高速です。

IEEE 802.1s で定義されている複数のスパニング・ツリー・プロトコル(MSTP)では、複数の VLAN をシングル STP インスタンスによって管理でき、VLAN 単位の STP をサポートします。結果として、複数の VLAN が少数のスパニング・ツリー・インスタンスにマッピングできます。これにより、類似のレイヤ 2 トポロジをもつ複数の VLAN に対してループ・フリーなトポロジを保証します。プロセードの実装では、MSTP が有効なブリッジにおいて 16 までのスパニング・ツリー・インスタンスをサポートします。つまり、16 の異なるレイヤ 2 トポロジをサポートします。MSTP を使用したスパニング・ツリー・アルゴリズムは高速な収束を提供する RSTP です。

BPDU ガード

STP 環境では、スイッチ、エンド・ステーション及びその他のレイヤ 2 デバイスは、ブリッジ・プロトコル・データ・ユニット (BPDU)を STP がデータ・フローに対する最適パスを決定するために使用します。STP の拡張機能の BPDU ガードは、ネットワーク内に BPDU を反映するノードを排除します。この機能は、STP ドメインの境界を強制し、BPDU ガードが有効なポートをもつネットワーク機器が STP の参加することを許可させないことにより、アクティブなトポロジを予測できるように制御します。たとえば、STP トポロジの変更において、エンド・ステーションなどの接続機器が STP に参加する必要がありません。このケースにおいては、エンド・ステーションが接続されたプロセードのポート上に STP BPDU ガードを有効にできます。STP BPDU ガードは、ポートをシャットダウンさせ、errdisable 状態にさせます。これにより、STP トポロジに接続機器が参加することができなくなります。BPDU ガードに抵触すると、ログ・メッセージが生成されます。設定が無効になったことを警告するネットワーク管理者への CLI メッセージが表示されます。BPDU ガード機能は、errdisable が解消しない場合、管理者が手動でインタフェイスを復旧させないといけないので 無効な設定に対する確実な対応を提供します。

STP BPDU ガードを個々のインタフェイスに有効にします(この機能は、デフォルトで無効です)。設定例は、以下のとおりです:

```
FastIron(config) interface ethe 2/1
FastIron(config-if-e1000-2/1) #stp-bpdu-guard
```

複数のポートに、この機能を一度に有効にするために、複数のインタフェイスを指定してコマンドを実行できます。:

```
FastIron(config)#interface ethernet 1/1 to 1/9
FastIron(config-mif-1/1-1/9) #stp-bpdu-guard
```

LLDP

リンク・レイヤ検知プロトコル (LLDP)は、IEEE 802.1AB 規格、ステーション及び MAC 接続性検知に記述されているレイヤ 2 ネットワーク検知プロトコルです。このプロトコルにより、IEEE 802 LAN/MAN に接続されたステーションは、LLDP のケータビリティを同じ 802 LAN セグメント内の他の LLDP が有効なステーションに広告し、検知することができます。

LLDP の広告によって伝播された情報は、たとえば SNMP プロトコルのような管理プロトコルを使用して NMS でアクセス可能な受信デバイスによって標準 MIB に保存されます。その情報はまた、`show lldp` コマンドを使用して、CLI から閲覧できます。

デュアル・モードの VLAN ポート

デュアル・モードのポートとしてタグ・ポートを設定することで、タグ・ポートのトラフィック及びアンタグ・ポートのトラフィックを同時に送受信できます。デュアル・モードのポートはそのポートに対して設定した VLAN 及びデフォルト・VLAN(つまり、アンタグのトラフィック)に属しているフレームを送受信します。

たとえば、下図に示すとおり、ポート 2/11 は VLAN20 に属しているデュアル・モードのポートです。VLAN20 及びデフォルト VLAN に対するトラフィックは、ハブからこのポートに流れます。デュアル・モードの機能により、VLAN20 に対するトラフィック及びアンタグのトラフィックが同時に対象ポートを通過できます。

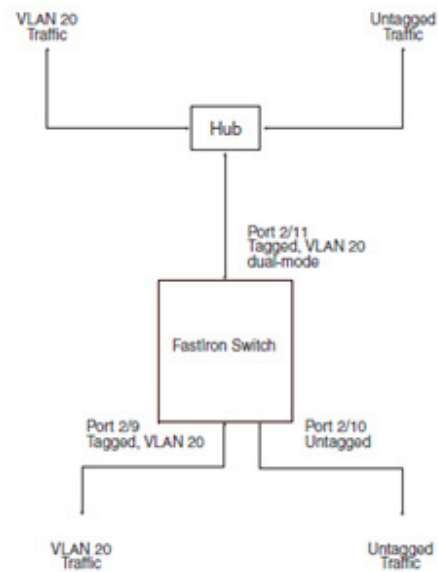


図 8: デュアル・モードの VLAN ポート

上記の例で、ポート 2/11 で、デュアル・モード機能を有効にするには、以下のコマンドを入力します:

```
FastIron(config)#vlan 20
FastIron(config-vlan-20)#tagged e 2/11
FastIron(config-vlan-20)#tagged e 2/9
FastIron(config-vlan-20)#int e 2/11
FastIron(config-if-e1000-2/11)#dual-mode
```

デュアル・モードのポートに対するデフォルトの VLAN ID の指定:

図で示しているとおり、タグ付きの他の VLAN に対してトラフィックを送信する一方で、デフォルト VLAN と異なる指定の VLAN に対するトラフィックを送信するために、デュアル・モードのポートをアンタグとして設定できます:

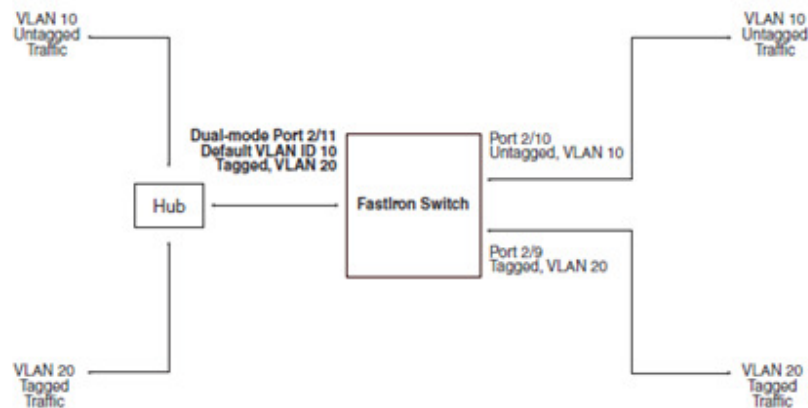


図 9: デュアル・モードのポート

このダイアグラムから、タグ・ポート 2/11 が VLAN10 及び VLAN20 に属しているデュアル・モードのポートであることがわかります。デュアル・モードのポートに割り当てられたデフォルト VLAN は 10 です。これは、ポート 2/11 が VLAN20(及び、該当ポートが属するすべての他の VLAN)上で、タグ付きのトラフィック及び VLAN10 上で、アンタグのトラフィックを送信することを意味します。

デュアル・モード機能により VLAN20 に対するタグ付きのトラフィック及び VLAN10 に対するアンタグのトラフィックが同時にポート 2/11 を通過することができます。デュアル・モードのポートは、アンタグのトラフィックのみをデフォルト VLAN(つまり、VLAN1 またはユーザが定義した VLAN ID)上で送信し、すべての他の VLAN 上でタグ付きのトラフィックのみを送信します。

次に示すコマンドは、図 10 に基づいて VLAN10 及び VLAN20 を設定しています。タグ・ポート 2/11 を、VLAN10 及び VLAN20 に追加した後、ユーザが定義したデフォルト VLAN10 のデュアル・モードを指定します。この設定では、ポート 2/11 は、VLAN10 上でアンタグのトラフィックのみを、VLAN20 上で、タグ付きのトラフィックのみを送信します。

```
FastIron(config)#vlan 10 by port
FastIron(config-vlan-10)#untagged e 2/10
FastIron(config-vlan-10)#tagged e 2/11
FastIron(config-vlan-10)#exit
FastIron(config)#vlan 20 by port
FastIron(config-vlan-20)#tagged e 2/9
FastIron(config-vlan-20)#tagged e 2/11
FastIron(config-vlan-20)#exit
FastIron(config)#int e 2/11
FastIron(config-if-e1000-2/11)#dual-mode 10
```

注記:

- デュアル・モードのコマンドで<vlan-id>を指定しない場合、そのポートのデフォルト VLAN は、1 に設定されます。そのポートは、デフォルト VLAN 上でアンタグのトラフィックを送信します。
- デュアル・モード機能は、デフォルトでは無効です。タグ付きのポートのみがデュアル・モードのポートとして設定できます。
- トランク・グループにおいて、すべてのポートはデュアル・モードでなければならない、または、どのポートもデュアル・モードになることができません。show vlan コマンドは、各 VLAN 上のデュアル・モードのポートに対して個別の列を表示します。

- 各ポート・ベース VLAN はタグまたはアンタグのポートから成ります。ポートがタグ付きでなければ、ポートは 1 つ以上のポート・ベース VLAN のメンバになれません。802.1Q タギングにより、ポートは、ポート上に送信された各パケットに対して VLAN ID を含む 4 バイトのタグ・フィールドを追加できます。
- また、VLAN 内のポートをタグ付けすることによって複数のデバイスを跨ぐポート・ベース VLAN を設定できます。

タグにより、パケットを受信する各デバイスがパケットの属する VLAN を決定することができます。

802.1Q タギングは、レイヤ 2 の VLAN のみに適用され、レイヤ 3 VLAN には適用されません。以下に設定例を示します：

```
FastIron(config)#vlan 4
FastIron(config-vlan-4)#untag e 3 to 4
FastIron(config-vlan-4)#tagged e 5
FastIron(config-vlan-4)#exit
FastIron(config)#vlan 10
FastIron(config-vlan-4)#untag e 8 to 9
FastIron(config-vlan-4)#tagged e 5
```

- レイヤ 3 プロトコル VLAN – 指定のプロトコル・タイプの共通かつ排他的なレイヤ 3 ブロードキャスト・ドメインを共有するポート・ベース VLAN 内のポートのサブセット。ポート・ベース VLAN 内のいくつか、またはすべてのポートをレイヤ 3 プロトコルに従ってまとめたい場合、ポート・ベース VLAN 内でレイヤ 3 ポート・ベース VLAN を設定しなければなりません。ポート・ベース VLAN 内でそれぞれ次に示すポート・ベース VLAN のタイプを設定できます。レイヤ 3 VLAN 内のすべてのポートは同じレイヤ 2 VLAN になければなりません。
- IP サブネット VLAN – 指定の IP サブネットの共通かつ排他的なサブネットのブロードキャスト・ドメインを共有するポート・ベース VLAN 内のポートのサブセット。
- IPv6 VLAN – IPv6 パケットに対する共通かつ排他的なサブネットのブロードキャスト・ドメインを共有するポート・ベース VLAN 内のポートのサブセット。
- IPX network VLAN – 指定の IPX ネットワークに対する共通かつ排他的なサブネットのブロードキャスト・ドメインを共有するポート・ベース VLAN 内のポートのサブセット
- AppleTalk ケーブル VLAN – 指定の AppleTalk ケーブル範囲に対する共通かつ排他的なサブネットのブロードキャスト・ドメインを共有するポート・ベース VLAN 内のポートのサブセット。

プライベート VLAN

プライベート VLAN は、標準レイヤ 2 ポート・ベース VLAN の特性をもちながら、さらに VLAN 上のフラッディング・パケットを制御します。以下の図は、プライベート VLAN を使用しているアプリケーションの例です。

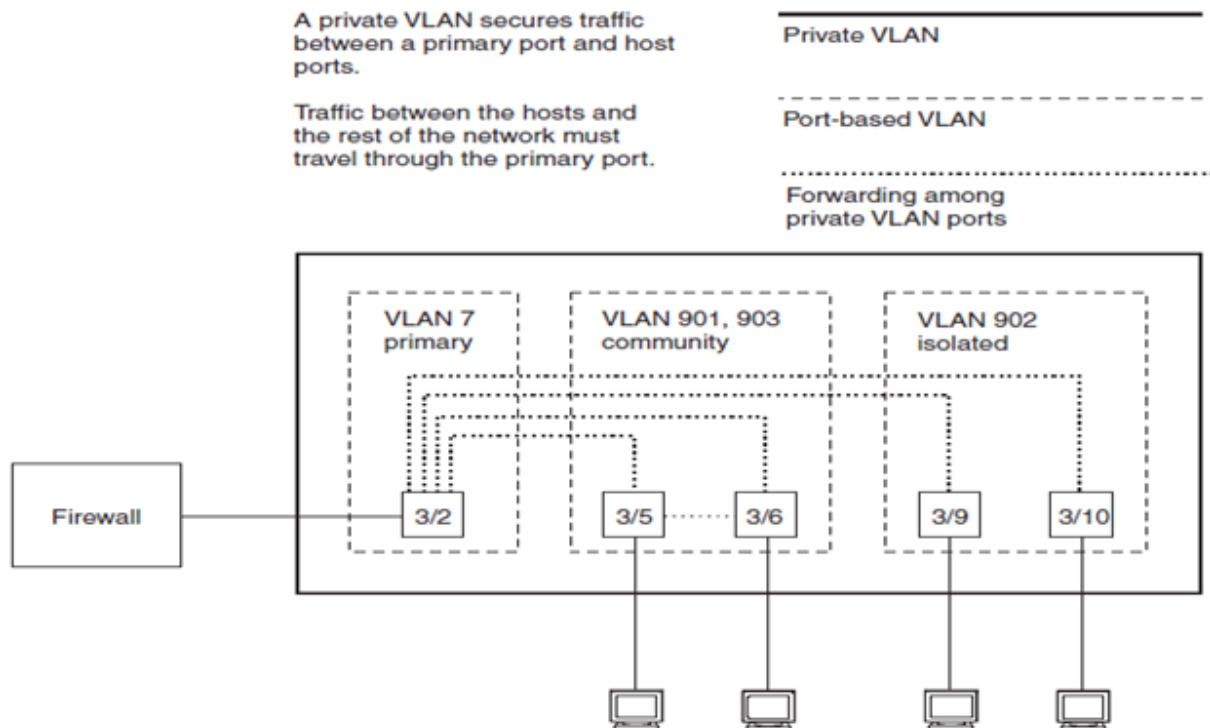


図 11: プライベート VLAN

この例では、プライベート VLAN を使用して、ファイアウォールを通過するネットワークとホスト間トラフィックの安全を確保します。上図のとおり、5 つのポートがプライベート VLAN のメンバです。最初のポート(ポート 3/2)は、ファイアウォールに接続されています。残りの 4 つのポート (ポート 3/5、3/6、3/9 及び 3/10)は、ファイアウォールに依存したホストに接続され、ネットワークとホスト間トラフィックの安全を確保します。ポート 3/5 及び 3/6 上の 2 つのホストはコミュニティ・プライベート VLAN 内で、ファイアウォール経由の通信と同様に、お互いに通信できます。ポート 3/9 及び 3/10 上の他の 2 つのホストは、独立(Isolated)VLAN 内で、ファイアウォール経由のみで通信ができます。2 つのホストは、同じ VLAN 内でもお互いに通信できないようにセキュリティが保たれています。

デフォルトでは、プライベート VLAN は、ブロードキャストまたは不明のユニキャスト(Unknown-unicast)のパケットを外部の送信元からプライベート VLAN へ転送しません。必要なら、ブロードキャスト及び、不明のユニキャストまたはその両方に対する動作を上書きできます。

以下に示すプライベート VLAN のタイプを組み合わせて設定できます:

- プライマリ- プライマリ・プライベート VLAN のポートは、“プロミスキャスト”で、ネットワーク上の自分宛以外のパケットも受信します。プロミスキャストポートにマッピングされた、独立及びコミュニティ VLAN すべての独立プライベート VLAN のポート及びコミュニティ・プライベート VLAN のポートと通信できます。
- 独立(Isolated) - 独立ポート上で受信したブロードキャスト及び不明ユニキャストは、プライマリ・ポートにのみ送信されません。独立 VLAN 内の他のポートへはフラッディングされません。

- コミュニティ- コミュニティ・ポート上で受信したブロードキャスト及び不明ユニキャストは、プライマリ・ポートへ送信され、また、コミュニティ VLAN 内の他のポートへフラッディングされます。

各プライベート VLAN は、プライマリ VLAN をもたなければなりません。プライマリ VLAN は、ネットワークとセキュアなポート間のインタフェイスです。プライベート VLAN は、コミュニティ VLAN と独立 VLAN を自由に組み合わせられます。

以下の表は、プライベート VLAN と標準のポート・ベース VLAN を比較しています:

フォワーディングの動作	プライベート VLAN	標準のポート・ベース VLAN
VLAN 内のすべてのポートが共通のブロードキャストを構成	構成しない	構成する
ブロードキャスト及び不明ユニキャストはすべての VLAN へ転送	転送しない(独立 VLAN) 転送する(コミュニティ VLAN)	転送する
既知のユニキャスト	転送する	転送する

7- モニタリング、メンテナンス、トラブルシューティング

OSPF 外部ルートの集約

レイヤ 3 スイッチが OSPF の ASBR(Autonomous System Boundary Router)であるとき、特定のアドレス範囲の経路を集約ルートされた、ひとつの外部ルートとして広告するように設定できます。

アドレス範囲を設定すると、すぐに有効になります。すべてのインポートされたルートは設定したアドレス範囲にしたがって、集約されます。すでに広告され、かつ、その範囲内にあるインポートされたルートは、その AS から消え、その範囲に相当する単一ルートが広告されます。

設定したアドレス範囲内のあるルートがレイヤ 3 スイッチによってインポートされる、レイヤ 3 スイッチがすでに集約ルートを広告している場合、新たにルート集約のアクションは行われません。もし集約ルートが広報されていないと、レイヤ 3 スイッチは集約ルートを広告します。もしアドレス範囲を指定してインポートされたルートがレイヤ 3 スイッチから削除され、なおかつ、同じアドレス範囲内を指定した他にインポートされたルートがある場合、新たにルート集約のアクションは行われません。もしインポートされたルートがない場合、集約ルートは削除されます。

集約ルートは、32 のアドレス範囲まで設定できます。レイヤ 3 スイッチは集約ルートの転送アドレスを 0 にセットし、そのタグを 0 にセットします。もしアドレス範囲を削除する場合、広告された集約ルートが消され、その範囲内のすべてのインポートされたルートが個々に広告されます。

外部 LSDB オーバフロー状態が発生する場合、すべての集約ルートは他の外部ルートとともに AS から消されます。レイヤ 3 スイッチが外部 LSDP オーバフロー状態でなくなると、すべてのインポートされたルートは設定したアドレス範囲にしたがって集約されます。

アドレス範囲に追加で再配布のフィルタを使用した場合、レイヤ 3 スイッチは再配布のフィルタをルートに適用し、その後アドレス範囲に適用することに注意してください。また、再配布を無効にした場合、すべての集約ルートは他のインポートされたルートと一緒に削除されることにも注意してください。

OSPF に対する集約アドレスを設定するためには、以下のようなコマンドを入力してください。

```
FastIron(config-ospf-router)#summary-address 10.1.0.0 255.255.0.0
```

この例にあるコマンドは集約アドレス、10.1.0.0 を設定しており、アドレス 10.1.1.0、10.1.2.0、10.1.3.0 などを含んでいます。これらすべてのネットワークに対して、10.1.0.0 のみが外部 LSA で広告されます。

OSPF 内部ルートの集約

ABR 上のエリアに対してアドレス範囲をオプションで割り当てます。アドレス範囲内のすべてのアドレスではなく、参照されるアドレス範囲だけがネットワークに広告されるため、エリア内で使用しているアドレス範囲を示す、特定の IP アドレスとマスク設定できます。各エリアは最大 32 のアドレス範囲を設定できます。

たとえば、193.45.5.1と193.45.6.2のサブネットに対してエリア範囲を定義するには、ABRで以下のコマンドを入力してください:

```
FastIron(config)#router ospf
FastIron(config-ospf-router)#area 1 range 193.45.0.0 255.255.0.0
```

Syntax: area <num> | <ip-addr> range <ip-addr> <ip-mask>

area <num> | <ip-addr> パラメータは、エリア番号を指定し、その内部の特定のネットワークが集約されます。range <ip-addr> パラメータは、その範囲内の IP アドレスの一部を指定します。ソフトウェアはアドレスとマスク内の最上位のビットを比較します。この比較により一致したすべてのネットワーク・アドレスはルータによって広告される単一ルートに集約されます。<ip-mask> パラメータは、あるルートが含む、集約ルートに集約される IP アドレスの一部を指定します。上記の例では、193.45 で始まるすべてのネットワークは、単一ルートに集約されます。

BGP ルート・フラップ・ダンペニング

“ルート・フラップ”は、ルートの状態がアップからダウン、または、ダウンからアップに変化することです。ルートの状態が変化したとき、状態の変化は、そのルートを維持するルータのルーティング・テーブル変更の原因となります。ルート状態が頻繁に変更すると、インターネットの不安定を引き起こし、そのルートを維持するルータに過度の処理が加わります。

ルート・ラップ・ダンペニングは、ルート状態の変化に対して BGP4 ルータの対応を変更することによって、そのルート・フラップのインパクトを減少させるメカニズムです。ルート・フラップ・ダンペニングを設定すると、レイヤ 3 スイッチは、許容できる安定したレベルを十分満たすように、そのルートの状態変化が減少するまで不安定なルートを抑制できます。

ルート・ラップ・ダンペニングはデフォルトでは無効です。ルートマップを使用して個々のルートを、またはグローバルでこの機能を有効できます。レイヤ 3 スイッチは、eBGP ネイバから学習したルートに対してのみ、ルート・ラップ・ダンペニングを適用します。

ルート・ラップ・ダンペニングのメカニズムは、ペナルティをベースにしています。あるルートが設定したペナルティ値を超えた場合、レイヤ 3 スイッチはそのルートの使用を停止し、他のルートへのアドバタイズも停止します。このメカニズムは、ルートの安定度が向上した場合、そのルートのペナルティを経時的に減らします。ルート・ラップ・ダンペニングのメカニズムは、以下のパラメータを使用します

:

- 抑制値 (Suppression threshold)
- 半減期 (Half-Time)
- 再利用値 (Reuse Threshold)
- 最大抑制時間 (Maximum suppression time)

ルート・ラップ・ダンピングの状態とすべてのダンピングされたルートを確認するためには、以下のコマンドを入力してください:

```
FastIron#show ip bgp flap-statistics
Total number of flapping routes: 414
Status Code >:best d:damped h:history *:valid
Network      From   Flaps Since  Reuse  Path
h> 192.50.206.0/23 166.90.213.771 0 :0 :13 0 :0 :0 65001 4355 1 701 h>
203.255.192.0/20 166.90.213.771 0 :0 :13 0 :0 :0 65001 4355 1 7018 h>
203.252.165.0/24 166.90.213.771 0 :0 :13 0 :0 :0 65001 4355 1 7018 h>
192.50.208.0/23 166.90.213.771 0 :0 :13 0 :0 :0 65001 4355 1 701 h>
133.33.0.0/16 166.90.213.771 0 :0 :13 0 :0 :0 65001 4355 1 701
*> 204.17.220.0/24 166.90.213.771 0 :1 :4 0 :0 :0 65001 4355 701 62
```

上記の出力の各フィールドの説明を以下に示します:

- Total number of flapping routes: レイヤ 3 スイッチ上で、これまで変更のあり、フラッピング・ルートとして選ばれた BGP4 のルート・テーブルの合計数
- Status code: ルートのダンピング状態は以下のいずれかになります:
 - > - BGP4 ルート・テーブル内のルート・ディスティネーションに対するベスト・ルート
 - d - 現在ダンピングされて、使用できないルート
 - h - 過去フラッピングして、現在到達性がないルート
 - * - 過去にフラッピングして、現在使用できるルート
- Network: ルートのディスティネーション・ネットワーク
- From: このレイヤ 3 スイッチにルートを送信したネイバ・ルータ
- Flaps: ルートがこれまでに、フラップ(状態変化)した数
- Since: 該当ルートが最初にフラップしてからの経過時間
- Reuse: 該当ルートが抑制されなくなり再利用されるまでの残時間
- Path: 該当ルートに対する AS パス情報

OSPF ネットワーク・タイプと DR/BDR の選出

複数のルータが接続されたネットワークでは、OSPF は、1 台のルータ DR として、同一セグメントにある、もう 1 台のルータを BDR として選出します。この DR/BDR の選出は、ネットワーク上の更新を転送する責任を負う DR 及び BDR へすべてのメッセージを転送することによって、ネットワーク上に繰り返し転送される情報を、最小限にします。

DR 及び BDR がまだ存在しないネットワークでは、最も高いプライオリティをもつネイバ・ルータが DR として、次に高いプライオリティをもつルータが BDR として選出されます。DR がオフラインとなる場合、BDR は自動的に DR になり、次に高いプライオリティをもつルータが新たに BDR になります。同じプライオリティのルータがある場合は、もっとも大きいルータ ID をもつルータが DR に指定され、ルータ ID が次に大きいルータが BDR として指定されます。同じネットワークの複数ルータが DR を宣言しているときは、プライオリティ及びルータ ID の双方が DR 及び BDR 選出に使用されます。他より高いプライオリティまたはより大きいルータ ID をもつネイバ・ルータが存在するにも関わらず、一台のルータのみが DR として既に選出されているとき、このルータは DR であり続けます。これは BDR に関しても同様です。

OSPF プロセスで重要なもののひとつは、隣接関係(*Adjacency*)です。隣接関係は、ルーティング情報を交換するためにネイバ・ルータ間で形成されるときに発生します。隣接関係にある OSPF のネイバ・ルータは、シンプルなヘロー・パケットの交換を行い、データベース情報を交換します。特定のセグメント上で情報交換を最小限にするために、隣接関係を形成する上での最初のステップのひとつは、DR 及び BDR を割り当てることです。DR は、コンタクト・ポイントの中心になります。それによって、マルチアクセス・セグメント内の収束を改善します。

OSPF の単一ペア間でレイヤ 3 の直接接続がある、OSPF のポイント・ツー・ポイントのネットワークにおいて、OSPF のマルチアクセスのネットワークで存在する DR 及び BDR は必要ありません。DR 及び BDR が不要なので、ポイント・ツー・ポイントの OSPF 隣接関係の形成と収束の処理をより速く実現します。ネイバ・ルータは、直接情報交換できるときはいつでも隣接関係を形成します。それとは対照的に、ブロードキャスト及びブロードキャストではないマルチアクセスのネットワーク(NBMA)において、DR 及び BDR はネットワークに接続されたすべての他のルータと隣接関係を形成します。

OSPF は、次のネットワーク・タイプをサポートします: ブロードキャスト、ポイント・ツー・ポイント、ポイント・ツー・マルチポイント及び NBMA。

OSPF インタフェイス: パッシブ及び無視(Ignore)

インタフェイスを OSPF パッシブまたは無視として設定するためには、次のコマンドをインタフェイスで使用してください:

```
[no] ip address <ip-addr>/<mask-bits> [ospf-ignore | ospf-passive | secondary]
```

`ospf-ignore` | `ospf-passive` パラメータは、レイヤ 3 のデフォルトの隣接関係の形成及びインタフェイスの広告に対するレイヤ 3 のでデフォルトを変更します。マルチ IP サブネットのアドレスをインタフェイス上で設定し、サブネットの一部で OSPF の動作を止めたい場合に、このパラメータのいずれかを使用します。:

- `ospf-passive` - このオプションは OSPF ネイバの隣接関係の形成を無効にします。デフォルトでは、OSPF が有効なインタフェイスでは、ソフトウェアは、そのインタフェイス上の各プライマリ IP アドレス及びインタフェイスに接続された OSPF ネイバ間で OSPF ルータの隣接関係を形成します。
- `ospf-ignore` - このオプションは、OSPF の隣接関係の形成を無効にし、また、そのインタフェイスの OSPF への広告を無効にします。これによって、そのサブネットは完全に OSPF から無視されます。

OSPF インタフェイスをパッシブに設定するとき、そのインタフェイスは OSPF ルートの更新を送受信しません。デフォルトでは、すべての OSPF インタフェイスはアクティブで、OSPF ルート情報を送受信できます。パッシブ・インタフェイスは、ルート情報を送受信しないため、そのインタフェイスはスタブネットワークとして動作します。このオプションは、インタフェイス上に設定されたすべての IP サブネットに影響することに注意してください。`ospf-passive` オプションは、隣接関係の形成を無効にしますが、インタフェイスの OSPF への広告を無効にしません。この広告を無効化し、隣接関係も無効にするには、`ospf-ignore` オプションを使用しなければなりません。

BGP ルートの動的更新と BGP ポリシ変更の適用

BGP ネイバからのすべてのルートを動的に更新するためには、以下のコマンドを入力してください:

```
FastIron(config-bgp-router)#clear ip bgp neighbor 192.168.1.170 soft in
```

このコマンドは、ネイバに BGP4 のテーブル(Adj-RIB-Out)の再送信を要求します。レイヤ 3 スイッチは、受信ルートにフィルタを適用し、必要に応じて BGP4 ルートを追加、変更、削除します。

Syntax: clear ip bgp neighbor all|<ip-addr>|<peer-group-name>|<as-num> [soft-outbound |soft[in|out]]

all | <ip-addr> | <peer-group-name> | <as-num> に対してネイバを指定します。

<ip-addr> パラメータは、レイヤ 3 スイッチの IP インタフェイスのネイバを指定します。

<peer-group-name> 指定のピア・グループ内のすべてのネイバを指定します。

<as-num> パラメータは、指定の AS 内のすべてのネイバを指定します。

<all> パラメータは、すべてのネイバ指定を意味します。

soft-outbound パラメータは、新しいまたは変更したフィルタを適用することによってすべての出力ルートを更新しますが、新規のまたは変更したフィルタによって影響を受けた既存のルートのみをそのネイバに送信します。

soft [in | out] パラメータは、ネイバから受信したルートまたは、ネイバへ送信したルートの更新かを指定します:

- soft in: 以下のいずれかになります:
 - ネイバまたはピア・グループに対して「soft reconfiguration」を有効にした場合、ルート・ポリシーを比較することによって、レイヤ 3 スイッチに保存されたルートの更新に対して、そのルートを更新します。「soft reconfiguration」はネイバからの追加の更新を要求しません。この設定がない場合、ネイバとの BGP セッションに影響します。
 - 「soft reconfiguration」を有効にしない場合は、そのネイバに BGP4 ルート・テーブル全体(Adj-RIB-Out)を要求し、フィルタを適用して、ルートを追加、変更、除外します。
 - ネイバが動的更新(Dynamic Refresh(をサポートしない場合は、「soft in」はネイバのセッションをリセットします。
- soft out: フィルタによって影響を受けたルートを変更または除外した後、すべてのアウトバウンド・ルートを更新し、レイヤ 3 スイッチの BGP4 ルート・テーブル(Adj-RIB-Out)全体をネイバに送信します。「in」や「out」を指定しない場合、レイヤ 3 スイッチは「in」及び「out」の双方のオプションを実行します。

soft-outbound パラメータは、新規のまたは変更したフィルタを適用することによって、すべてのアウトバウンド・ルートを更新しますが、新規のまたは変更したフィルタによって影響を受けた既存のルートのみをネイバに送信します。

「soft out」パラメータは、すべてのアウトバウンド・ルートを更新し、フィルタによって影響を受ける新規のまたは変更したフィルタによって影響を受けた既存のルートを変更または除外した後、レイヤ 3 スイッチの BGP4 ルート・テーブル (Adj-RIB-Out) 全体をネイバに送信します。

すべてのレイヤ 3 スイッチの BGP ルート・テーブルを動的にネイバへ再送するためには、以下のコマンドを入力します:

```
FastIron(config-bgp-router)#clear ip bgp neighbor 192.168.1.170 soft out
```

このコマンドはレイヤ 3 スイッチの BGP4 ルート・テーブル(Adj-RIB-Out)に送信ルートに対するフィルタを適用し、適宜ルートを変更または除外した後、ネイバに、Adj-RIB-Out の結果を送信します

プロケードのレイヤ 3 スイッチは、ネイバのセッションがアップ・ダウンするとき、新規のまたは変更したアウトバウンドのポリシーまたはフィルタを使用しているアウトバウンド・ルートを自動的に更新しません。それに代わり、レイヤ 3 スイッチは、あるルートがアウトバウンドのキュー (Adj-RIB-Out) に登録されるとき、新規のまたは変更したポリシーまたはフィルタを適用します。新規のまたは変更したポリシーまたはフィルタを有効にするためには、ネイバとのセッションがアップ・ダウンするかどうかに関係なく、「clear ip bgp neighbor」コマンドを入力しなければなりません。オプションなしでこのコマンドを入力するか、「soft out」または「soft-outbound」オプションを入力できます。いずれかの方法に加え、ネイバに対して、`<ip-addr>`、`<as-num>`、`<peer-group-name>` または `all` のいずれかのパラメータを指定しなければなりません。

ポリシー変更を有効にするためには、以下のコマンドを入力します:

```
FastIron(config-bgp-router)#clear ip bgp neighbor 10.10.200.102 soft in
```

このコマンドは、BGP ピアのセッションを切断しません。レイヤ 3 スイッチが保持しているルートの更新に対するルートのポリシーを比較することによって、そのルートを更新します。また、このコマンドは、ネイバからの追加の更新を要求しません。その更新を要求する場合は、ネイバとのセッションに影響を及ぼします。「in」を指定しない場合、このコマンドは、インバウンドとアウトバウンドの双方に適用されます。以下のセクションでは、新規のまたは変更したフィルタを有効にするために、どのように BGP4 ルートを動的に更新するかを記述しています。

BGP4 セッションの切断と再確立することで、全ての BGP ルートをネイバに再送する場合には、「clear ip bgp neighbor x.x.x.x or clear ip bgp neighbor all」を実行します。

The following sections describe how to dynamically refresh BGP4 routes to place new or changed filters into effect. If you need to tear down and re-establish the BGP session and resend all BGP routes between neighbors, use the hard clear command `clear ip bgp neighbor x.x.x.x or clear ip bgp neighbor all`.

より多くの VLAN または仮想ルーティング・インタフェイスに対するメモリの割り当て

プロケードのレイヤ 2 及びレイヤ 3 スイッチは、4,095 まで VLAN をサポートします。さらに、レイヤ 3 スイッチは、512 まで仮想ルーティング・インタフェイスをサポートします。プロケードの製品でサポートされる VLAN 数及び仮想ルーティング・インタフェイスは、デバイスに依存し、シャーシにおいては、マネジメント・モジュール上の DRAM 数に依存します。以下の表は、レイヤ 2 及びレイヤ 3 スイッチに対する VLAN 及び仮想ルーティング・インタフェイスのデフォルトの最大数及び設定できる最大数を示しています:

VLAN		仮想ルーティング・インタフェイス	
デフォルトの最大数	設定できる最大数	デフォルトの最大数	設定できる最大数
64	4094	255	512

表 3: VLAN 及び仮想ルーティング・インタフェイスの最大値

設定できる VLAN 数を増加させる場合、4,095 まで VLAN を指定できますが、設定できる VLAN は、4,094 までです。4,094 の VLAN ID はシングル・スパンニング・ツリー機能による使用で予約されています。設定できる VLAN 最大数を増加させるには、次のコマンドを入力します:

```
FastIron(config)#system-max vlan 2048
FastIron#reload
```

設定できる仮想ルーティング・インタフェイスの最大数を増加させるには、次のコマンドを入力します:

```
FastIron(config)#system-max virtual-interface 512
FastIron#reload
```

ログに対する OSPF の Syslog メッセージの指定

OSPF 関連の Syslog メッセージのどのタイプをログに記録するかを指定できます。デフォルトでは、ログに記録される OSPF メッセージは、可能性のあるシステム・エラーを示しているメッセージです。その他の OSPF メッセージのタイプをログに記録したい場合、そのログを取得するように、ブロードのデバイスを設定できます。たとえば、すべての OSPF 関連の Syslog メッセージのログを記録するように指定する場合、次のコマンドを入力します:

```
FastIron(config)#router ospf
FastIron(config-ospf-router)#log all
```

Syntax: [no] log all | adjacency | bad_packet [checksum] | database | memory | retransmit

このログコマンドには、次のオプションがあります:

- all オプションは、すべての OSPF 関連の Syslog メッセージのログを取得します。「no log all」コマンドでこのオプションを後で無効にする場合、OSPF ログ・オプションは、デフォルトの設定に戻ります。
- adjacency オプションは、重要な OSPF ネイバ状態変化、特にエラーのケースに関するログを取得します。このオプションは、デフォルトでは無効です。
- bad_packet checksum オプションは、チェックサム・エラーをもつすべての OSPF パケットのログを取得します。このオプションは、デフォルトでは、有効です。
- bad_packet オプションは、すべての他の不正な OSPF パケットのログを取得します。このオプションは、デフォルトでは、無効です。
- database オプションは、OSPF の LSA 関連情報のログを取得します。このオプションは、デフォルトでは、無効です。
- memory オプションは、異常な OSPF のメモリ使用のログを取得します。このオプションは、デフォルトでは、有効です。
- retransmit オプションは、OSPF 再送 retransmission のログを取得します。このオプションは、デフォルトでは、無効です。

ポート・ミラーリング及びモニタリング

ポート・ミラーリングは、ネットワーク・スイッチ上のあるポートからパケットを分析する別のポートへ、各入出力のコピーを転送し、ネットワークのトラフィックをモニタリングする手法です。ポート・ミラーリングは、特に攻撃防止に対して診断ツールまたはデバッグ機能として使用できます。ポート・ミラーリングは、スイッチのローカルまたはリモートで管理できます。

すべてのパケットをコピーするポート及びそのコピーされたパケット (モニタ・ポート) が送信されるポート (ミラー・ポート) を割り当てることによってポート・ミラーリングを設定します。モニタ・ポート上の送受信パケットは、正常に転送され、またミラー・ポートへコピーされます。ミラー・ポート上にプロトコル・アナライザを接続します。アナライザは、ミラー・ポートのクライアントに影響を及ぼさずに、データをキャプチャし、評価します。

ブロードバンドのデバイス上の個々のポートで、ポート・ミラーリングを設定するには、次のようなコマンドを入力します:

```
FastIron(config)#mirror-port ethernet 1/2/4
FastIron(config)#interface ethernet 1/2/11
FastIron(config-if-e1000-11)#monitor ethernet 1/2/4 both
```

イーサネット・ポート 1/2/11 上のトラフィックは、モニタされ、モニタされたトラフィックは、ミラー・ポートのイーサネット・ポート 1/2/4 にコピーされます。

Syntax: [no] mirror-port ethernet [<stack-unit>/<slotnum>/]<portnum> [input | output]

Syntax: [no] monitor ethernet [<stack-unit>/<slotnum>/]<portnum> both | in | out

- ミラー・ポートのイーサネット<portnum> に対するパラメータは、モニタされたトラフィックがコピーされるポートを指定します。
- モニタ・ポートのイーサネット<portnum> に対するパラメータは、トラフィックがモニタされるポートを指定します。
- input 及び output パラメータは、入力または出カトラフィックに対して排他的に ミラー・ポートを設定します。いずれも指定しない場合、双方のタイプが適用されます。
- both, in 及び out パラメータは、ミラー・ポート上でモニタしたいトラフィックの方向を指定します。デフォルトの設定はありません。

ポート・ミラーリングの設定を表示するには、「show monitor」及び「show mirror」コマンドを入力します。また、ACL ベースの入力ミラーリング、MAC フィルタ・ベースのミラーリング及び VLAN ベースのミラーリングを設定できます。

SNMP

SNMP は、IP ネットワーク(サーバ、ワークステーション、ルータ、スイッチなど)を管理するために開発されたプロトコルです。現在は、3 つのバージョンがあり、SNMP v1、v2 及び v3 で定義されています。SNMP は、複雑なネットワークを管理するプロトコルのセットです。SNMP はプロトコル・データ・ユニット(PDU)と呼ばれるメッセージをネットワークの異なる部分へ送信します。エージェントと呼ばれる SNMP に準拠したデバイスは、管理情報ベース(MIB)内の自身のデータを保管し、SNMP リクエストに返送します。管理機能に安全にアクセスするために、ACL を使用して、特定の IP アドレスまたは VLAN への SNMP アクセスを制限できます。また、スイッチ上で SNMP アクセスも同様に無効にできます。

以下に SNMP アクセスを制御するために ACL を使用する例を示します:

```
FastIron(config)#access-list 25 deny host 209.157.22.98 log
FastIron(config)#access-list 25 deny 209.157.23.0 0.0.0.255 log
FastIron(config)#access-list 25 deny 209.157.24.0 0.0.0.255 log
FastIron(config)#access-list 25 permit any
FastIron(config)#access-list 30 deny 209.157.25.0 0.0.0.255 log
FastIron(config)#access-list 30 deny 209.157.26.0/24 log
FastIron(config)#access-list 30 permit any
FastIron(config)#snmp-server community public ro 25
FastIron(config)#snmp-server community private rw 30
```

「snmp-server community」が設定されると、すべての入力 SNMP パケットは最初にコミュニティ・ストリングによって確認され、それから、入力または出力方向の ACL によって確認されます。

Syntax: snmp-server community <string> ro | rw <num>

- <string> パラメータは、SNMP アクセスを得るために、ユーザが入力しなければならない SNMP コミュニティ・ストリングを指定します。
- ro パラメータは、コミュニティ・ストリングが読み取り("get")アクセスする場合に指定します。
- rw パラメータは、コミュニティ・ストリングが読み取り・書き込み("set")アクセスする場合に指定します。
- <num> パラメータは、1 から 99 までの標準 ACL 番号を指定します。上記のコマンドは、ACL 25 番及び 30 番を設定し、コミュニティ・ストリングにその ACL を適用します。ACL 25 番は、「public」コミュニティ・ストリングを使用して、読み取りアクセスを制御するために使用されます。ACL 30 は、「private」コミュニティ・ストリングを使用する読み取り・書き取りアクセスを制御するために使用されます。

SNMP バージョン 3 (SNMPv3)では、セキュリティ及びリモート設定の機能が、バージョン 2 に追加されています。SNMPv3 を使用すると、ユーザはデータの改ざんを恐れることなく、SNMP エージェントから管理情報を収集できます。また、デバイスの設定を変更する、「SNMP set」パケットのような機密情報を、ワイヤ上で漏洩の危険にさらされることから防止するために暗号化できます。さらに、グループ・ベースの管理モデルにより、異なるユーザは同じ SNMP エージェントに異なるアクセス権限をもってアクセスすることができます。SNMPv3 アーキテクチャは、メッセージのセキュリティに対するユーザ・ベースのセキュリティ・モデル(USM)及びアクセス制御に対するビュー・ベースのアクセス制御モデル(VACM)を提供します。このアーキテクチャは、たとえば、セキュリティ、認証とプライバシー、認証とアクセス制御、管理フレームワーク、エンティティのネーミング、ユーザとポリシー、ユーザ名とキー管理、通知の送信先、プロキシ関連、SNMP 操作によるリモート設定のような異なるセキュリティ、アクセス制御及びメッセージ処理モデルの同時接続の使用をサポートします。

SNMPv3 ではまた、エージェント設定を意味する MIB オブジェクトに対して、「SNMP set」コマンドを使用する SNMP エージェントを動的に設定することができます。この動的な設定のサポートにより、ローカルまたはリモートによるエントリの追加、削除及び変更設定ができます。

パスワード・リカバリ

パスワード・リカバリは、シリアル・コンソールへのダイレクト・アクセス及びシステムのリセットが必要です。パスワード・リカバリは、以下のステップに従ってください:

1. デバイスへのシリアル・インタフェースの CLI セッションを開始します。
2. デバイスを再起動します。
3. システム起動時の初期ブート・プロンプトで、ブート・モニタ・モードになるために、「b」を入力します。
4. このプロンプトで「no password」を入力します (このコマンドを省略することはできません)。このコマンドによりデバイスは、システムのパスワード確認をバイパスします。
5. このプロンプトで「boot system flash primary」を入力します。
6. コンソールのプロンプトが再び表示された後に、新しいパスワードを割り当てます。